DISEÑO DE UN SOFTWARE PROTOTIPO QUE PERMITA PARAMETRIZAR UN GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN

Ing. LIANA CAROLINA MONTAÑA CARPINTERO
Ing. JAVIER ALBERTO MONTAÑA CARPINTERO
Ing. DIANA TERESA VALENCIA PEDRAZA

Proyecto de Grado para optar al Título de
Especialista en Seguridad Informática

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA INGENIERÍA DE SISTEMAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, D.C.
2017

DISEÑO DE UN SOFTWARE PROTOTIPO QUE PERMITA PARAMETRIZAR UN GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN

Ing. LIANA CAROLINA MONTAÑA CARPINTERO
Ing. JAVIER ALBERTO MONTAÑA CARPINTERO
Ing. DIANA TERESA VALENCIA PEDRAZA

Proyecto de Grado para optar al Título de
Especialista en Seguridad Informática

Asesor: Ing Lorena Ocampo
Ing de Sistemas

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA INGENIERÍA DE SISTEMAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, D.C.
2017

Nota de Aceptación

Aprobado por los jurados de grado
Cumpliendo con los requisitos
Exigidos por la Universidad Piloto
de Colombia para optar al título de
Especialista en seguridad informática

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá, D.C., 7 de marzo de 2017

Dedicado a Dios por permitirnos culminar está etapa de nuestra formación profesional. A nuestras familias que son el pilar más importante en nuestras vidas y a todas aquellas personas que nos aportaron el conocimiento y experiencia en los temas que abordan este proyecto de grado.

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE CUADROS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

ACTIVOS: cualquier objeto de valor para la una organización o empresa constituida entre otros por los siguientes tipos[1]

- De información: Bases de datos, archivos, contratos y acuerdos, documentación de sistema, información de investigación, manuales de usuario, material de entrenamiento, procedimientos operacionales o de soporte, planes de Continuidad de Negocio, registros de auditoría, e información de archivo.

- De Software: aplicaciones, de sistema, herramientas de desarrollo y utilidades.

- Físicos: equipos de cómputo, equipos de comunicaciones, medios removibles y otros.

- Servicios: servicios computacionales y de comunicación, utilidades generales como calefacción, iluminación especial, energía y aire acondicionado.

- Personas: incluyendo sus calificaciones, competencias y experiencia.

- Intangibles: como reputación e imagen de la organización.

ADQUISICIÓN MANTENIMIENTO Y DESARROLLO DE SISTEMAS DE INFORMACIÓN: garantizar que la seguridad es parte integral de los sistemas de información. (Asegurar la inclusión de todos los controles de seguridad en los sistemas de información como infraestructura, aplicaciones, servicios, etc[2].) (Prezi.com, 2012)

AMENAZA: evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos de información.[3]

CONFIABILIDAD: la información debe ser la apropiada para la administración de la entidad y el cumplimiento de sus obligaciones[4].

---

[1] DEBITOORS. ¿Qué son activos? [En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://debitoor.es/glosario/definicion-de-activos.

[2] PREZI.CON. Significado de Adquisición, mantenimiento y desarrollo de sistemas de información. 2012. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://prezi.com/.../tema-7-adquisicion-desarrollo-y-mantenimiento-de-los-sistemas-d

[3] SEGURIDAD INFORMÁTICA. ¿Qué es amenaza informática? . [En línea], [consultado el 23 de octubre de 2016]. Disponible en: www.seguridad**informatica**.unlu.edu.ar

[4] SCRIBD. Definición de confiabilidad. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://es.scribd.com/doc/35643664/**Definicion**-de-**Confiabilidad**

CONFIDENCIALIDAD: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados[5].

CUMPLIMIENTO: garantizar la aplicación de las leyes, regulaciones y obligaciones contractuales a las cuales están sujetos los procesos de la Entidad.[6]

CONTROL DE ACCESO: controlar el acceso a la información. (Control físico o lógico de los accesos, áreas de procesamiento y procesos de la Organización.)[7]

CUMPLIMIENTO: evitar el incumplimiento total o parcial de cualquier ley, estatuto, regulación u obligación contractual de los requerimientos de seguridad.[8]

DISPONIBILIDAD: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.[9]

EFECTIVIDAD: la información relevante debe ser pertinente y su entrega oportuna, correcta y consistente[10].

EFICIENCIA: el procesamiento y suministro de información debe hacerse utilizando de la mejor manera posible los recursos[11].

EVALUACIÓN DE RIESGOS: la evaluación de las amenazas, impactos y vulnerabilidades relativos a la información y a las instalaciones de procesamiento de la misma, y a la probabilidad de que ocurran.[12]

EVENTO ADVERSO: es una situación o modificación observable dentro de un ambiente que ocurre en un periodo de tiempo, ó un estado específico o un cambio

---

[5] LA ORGANIZACIÓN INTERNACIONAL DE ESTANDARIZACIÓN. Tecnología de la información – técnicas de seguridad – código para la práctica de la gestión de la seguridad de la Información Estándar Internacional ISO/IEC 17799: .Comité Técnico Conjunto ISO/IEC JTC 1

[6] DEFINICIONES ABC ¿Qué es confidencialidad? [En línea], [consultado el 23 de octubre de 2016]. Disponible en: definicionABC.de/confidencialidad/

[7] TECNOSEGURO ¿Qué es un control de acceso? [En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://www.tecnoseguro.com/.../**control-de-acceso**/¿-que-es-un-**control-de-acceso**.htm.

[8] DEFINICIÓN MX. ¿Qué es cumplimiento? [En línea], [consultado el 23 de octubre de 2016]. Disponible en: definicion.mx/disponibilidad/

[9] DICCIONARIO CONTABLE. ¿Qué es disponibilidad? [En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://es.diccionariocontable.com/doc/35643664/**Definicion**-de-disponibilidad.

[10] DEFINICIÓN ABC. ¿Qué es efectividad? [En línea], [consultado el 23 de octubre de 2016]. Disponible en: www.definicionabc.com › General

[11] DEFINICIÓN ABC. ¿Qué es eficiencia? [En línea], [consultado el 23 de octubre de 2016]. Disponible en: definicionABC.de/eficiencia/

[12] ISTAS. ¿Qué es evaluación de riesgos? [En línea], [consultado el 23 de octubre de 2016]. Disponible en: www.istas.net/web/index.asp?idpagina=

de estado en un sistema ó red informática con consecuencia negativa que puede comprometer o compromete la confidencialidad, integridad o disponibilidad de la información; es decir, cualquier actividad que afecte o dañe los activos (redes y/o equipos de TI) de la organización o empresa[13].

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad[14].

GESTIÓN DE COMUNICACIONES Y OPERACIONES: asegurar la correcta y segura operación de los servicios de procesamiento de información (actividades operativas y concernientes a la plataforma tecnológica).[15]

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN: asegurar que los eventos de seguridad de la información y las debilidades asociadas con los sistemas de información, sean comunicadas de tal manera que se tome una acción correctiva adecuada en el momento indicado.[16]

GESTIÓN DE LA CONTINUIDAD DE NEGOCIO: contrarrestar las interrupciones a las actividades de la Organización y proteger sus procesos críticos contra los efectos de fallas mayores o desastres en los sistemas de información, y asegurar que se recuperen a tiempo[17].

GESTIÓN DEL RIESGO: el proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a los sistemas de información.[18]

GESTIÓN DE ACTIVOS DE INFORMACIÓN: lograr y mantener la protección apropiados de todos los activos de información[19].

---

[13] CGH. Eventos Adversos. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: www.cgh.org.co/imagenes/calidad1.pdf

[14] EVOLUTION IT. ¿Qué son eventos de la seguridad? [En línea], [consultado el 23 de octubre de 2016]. Disponible en: www.evolution-it.com.co/...**seguridad**/siem-**seguridad-de-la-informacion**

[15] MINISTERIO DEL INTERIOR. ¿Qué significa eventos de seguridad de la información? [En línea], [consultado el 23 de octubre de 2016]. Disponible en www.mininterior.gov.co/sites/.../OIP-2014-PSI-Especificas-5%20**Comunicaciones**.doc

[16] MINISTERIO DEL INTERIOR. Significado de gestión de comunicaciones y operaciones. . [En línea], [consultado el 23 de octubre de 2016]. Disponible en: www.mininterior.gov.co/sites/ .../OIP-2014-PSI-Especificas-5%20**Comunicaciones**.doc

[17] CERT. Gestión de incidentes de seguridad de la información. . [En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://www.cert.uy/.../politica+de+**gestion**+de+ **incidentes**+(.pdf+602+KB).pdf?.

[18] ICESI. ¿Qué es gestión del riesgo? [En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://www.icesi.edu.co/revistas/index.php/estudios_gerenciales/article/view/.../html

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: evento o serie de eventos adversos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones de la Organización y amenazar la seguridad de la información[20].

INTEGRIDAD: propiedad de salvaguardar la exactitud y estado completo de los activos[21].

POLÍTICA DE SEGURIDAD: apoya y orienta a la Alta Dirección con respecto a la seguridad de la información, de acuerdo con los requisitos de la organización o empresa, los reglamentos y las leyes pertinentes[22].

RIESGO INFORMÁTICO: Combinación de la Probabilidad de ocurrencia de un evento informático no esperado y sus posibles consecuencias.[23]

SEGURIDAD DE LA INFORMACIÓN: Es la preservación de la confidencialidad, integridad y disponibilidad de la información; además puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.[24]

SEGURIDAD ORGANIZACIONAL: gestiona la seguridad de la información dentro de la organización o empresa. Agrupa los temas de administración de la seguridad dentro de la organización. (Roles, compromisos, autorizaciones, acuerdos, manejo con terceros).[25]

---

[19] MINISTERIO DE TECNOLOGÍA, INDUSTRIA Y COMERCIO. Gestión de activos de información, [En línea], [consultado el 23 de octubre de 2016]. Disponible en: www.mintic.gov.co/**gestion**ti/615/articles-5482_G5_**Gestion**_Clasificacion.pdf

[20] CERT. Incidente de seguridad de la información: [En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://www.cert.uy/.../politica+de+gestion+de+ **incidentes**+ (.pdf+ 602+KB).pdf?.

[21] INFOSEGUR. ¿Qué es integridad? [En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://infosegur.wordpress.com/tag/**integridad**/

[22] UNIVERSIDAD DISTRITAL. ¿Qué son políticas de seguridad? En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://portalws.udistrital.edu.co/.../**politica_seguridad**/ .../**Política** _para_**Seguridad_I**

[23] SEG.INFORMÁTICOS. Qué son riesgos informáticos. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: seg **informatica**1audisistem.jimdo.com/**riesgos**-**informáticos**/

[24] PROTEJETE. ¿Qué es Seguridad de la información?, [En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://protejete.wordpress.com/gdr_principal/**seguridad_ información_ protección**/

[25] DIALNET. ¿Qué es seguridad organizacional? [En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://dialnet.unirioja.es/descarga/articulo/2498321.pdf

SEGURIDAD INFORMÁTICA: Medidas de protección contra riesgos inherentes a la plataforma informática y que pueden afectar la integridad, disponibilidad y confidencialidad de la información.[26]

SEGURIDAD DEL RECURSO HUMANO: establece los criterios para asegurar que empleados, contratistas y terceros entiendan sus responsabilidades y sean adecuados para los roles a desempeñar reduciendo los riesgos relacionados con el personal.[27]

SEGURIDAD FÍSICA Y DEL ENTORNO: hace énfasis en evitar el acceso físico no autorizado (perímetro), daños o interferencias a las instalaciones de la organización y a su información.

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. SGSI: parte del sistema de gestión global, basado en un enfoque hacia los riesgos globales de la organización, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.[28]

VULNERABILIDAD: debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.[29]

[26] GESTIOPOLIS. Seguridad informática. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: www.gestiopolis.com/procedimientos-de-**seguridad**-**informática**-en-sitios-web

[27] GOOGLE. Seguridad física y del entorno. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://sites.google.com/a/istpargentina.edu.pe/.../seguridad-fisica-y-del-entorno

[28] INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Sistema de Gestión de la Seguridad de la Información. ISO/IEC 27001:2013. Bogotá D.C. 2013. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: intranet.bogotaturismo.gov.co/ sites/intranet...gov.co/.../NTC-**ISO**-**IEC**%2027001 pdf

[29] CODEJOBS. Vulnerabilidad. [En línea], [consultado el 23 de octubre de 2016]. Disponible en:¿Qué es vulnerabilidad? https://www.codejobs.biz/.../seguridad-informática-que-es-una-vulnerabilidad- una-am.

RESUMEN

En este documento usted va a encontrar una propuesta de tesis orientada a la creación de un diseño de software prototipo que permita parametrizar un gobierno de seguridad de la información en cualquier tipo de empresa basado en la norma internacional iso 27001: 2014 y en el manual de preparación para la certificación CISM de Isaca en el gobierno de seguridad de la información.

El documento está estructurado de manera lógica iniciando por la definición del problema identificado y la correspondiente justificación en la cual se propone el desarrollo del prototipo de software para permitir a los altos directivos organizacionales tomar adecuadas y acertadas decisiones misionales orientadas a la seguridad de los activos de información**.** Así mismo se plantea en el documento un objetivo general y cinco objetivos específicos estos hacen parte fundamental de la metodología del ciclo de desarrollo de software y están compuestos de las siguientes fases: Análisis de los requerimientos, flujogramas - casos de uso, diseño de la base de datos, diseño del prototipo y pruebas estas últimas se han documentado con imágenes reales de los diferentes módulos que conforman el prototipo de software propuesto, las pruebas se realizaron con información real de una empresa dedicada a la venta, mantenimiento de tecnología, sistemas de cómputo y el desarrollo de software a la medida . El documento termina con resultados e impactos esperados, reportes y conclusiones.

INTRODUCCIÓN

Hoy en día, las empresas hacen uso de las tecnologías de la información para las actividades del negocio, usan, procesan transportan y difunden cualquier cantidad de información, digital o de otro tipo con diferentes finalidades, sin embargo, han descuidado la seguridad en todos los aspectos y a su vez olvidan que las organizaciones deben sujetarse a los marcos legales regulatorios dentro y fuera de las mismas.

Un gobierno de seguridad estructurado permitirá a cualquier organización tener un control adecuado de la información que maneja como también la identificación de los activos críticos de información los cuales son la base fundamental en la continuidad del negocio. Así mismo la organización podría identificar la gestión de riesgos y los controles para mitigar esos riesgos y de esta forma coadyuvar a las organizaciones a tomar las decisiones adecuadas y alinearlas con la misión y visión de la organización con el propósito de preservar los principios de confidencialidad (proteger los datos y la información intercambiada entre emisor y receptor frente a terceras personas), integridad (mantener los datos libres de modificaciones no autorizadas y la disponibilidad(asegura que se pueda acceder en cualquier momento a la información).[30]

En la medida que se vaya madurando la estructura del gobierno de seguridad dentro de la organización se puede ir planificando la inclusión de la inversión del presupuesto para la seguridad y satisfacer los recursos disponibles para las proyecciones de nuevas tecnologías basadas en seguridad todo alineado a la gestión del riesgo los objetivos organizacionales de los altos directivos.[31]Quienes tendrán una nueva manera de ver a la seguridad con un enfoque global que involucra infraestructura, personas y procesos.

Por medio del análisis diseño y programación de un prototipo de software para la Gestión de gobierno de seguridad y con los conceptos regulatorios de las normas ISO 27001:2013[32], ISO 27014 ISACA en el dominio del gobierno de seguridad se pretende permitir a las organizaciones evaluar, controlar, dirigir y comunicar de forma eficiente las actividades que están relacionadas con la información.[33]

---

[30] SEGURIDAD ANGGIE. Blog Seguridad informática. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: http://seguridadanggie.blogspot.com.co/2011/11/confidencialidad.html

[31] INFORMÁTICA BÁSICA. Lo que tienes que saber sección Magazine Impacto de las TI. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: http://informaticabasica28.blogspot.com. co/2013/03/impacto-de-las-ti.html>

[32]INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Sistema de Gestión de la Seguridad de la Información. ISO/IEC 27001:2013. Bogotá D.C. 2013

[33]SGSI. Blog especializado en sistemas de gestión de seguridad de la información ISO 2014 Gobernanza seguridad de la información 4 abril de 2014. : [En línea], [consultado el 23 de octubre

Finalmente se espera que el prototipo permita parametrizar los procesos, recursos, infraestructura de un gobierno de seguridad y abarque hasta el reconocimiento de los activos críticos de información de las organizaciones.

de 2016]. Disponible en: http://www.pmg-ssi.com/2014/04/iso-27014-gobernanza-de-seguridad-de-la-informacion/>

1. DEFINICION DEL PROBLEMA

Los altos directivos organizacionales piensan que con solo tener recursos tecnológicos a la mano están dándole flujo a la información, pero se olvidan que a esa información hay que protegerla como un activo crítico, tan es así que no le están dando el tratamiento adecuado y se percatan de ello en el momento en el cual la disponibilidad, integridad y confidencialidad de la información se ve comprometida y se obvian los marcos regulatorios estipulados por las leyes locales y regionales.

¿Permitirá a los altos directivos organizacionales tomar adecuadas y acertadas decisiones misionales?

2. JUSTIFICACIÓN

Actualmente existe Software especializado para el análisis de riesgos y escaneo de vulnerabilidades herramientas de hacking ético que asisten en la evaluación de la seguridad tanto de la información a distintos niveles como de los sistemas, redes de computadoras, aplicaciones Web y servidores, brindando ayuda a las organizaciones mediante pruebas de penetración.[34] y exploración de dichos sistemas, con la finalidad de conocer los riesgos de las intrusiones. Estas herramientas y software son indispensables y han sido creados para dar continuidad al negocio. Aunque la base fundamental en una organización es la implementación estratégica y estructurada de un Gobierno de seguridad, actualmente no se tienen referencias de prototipos de software que planteen un SGSI desde el gobierno de Seguridad basado en los niveles de gestión, alineación estratégica organizacional, definición de roles y responsabilidades, normatividad y aspectos regulatorios, así como la administración de recursos. El estudio de investigación que se propone es la creación de un prototipo basado en el diseño y planificación de un gobierno de seguridad efectivo que sea la base fundamental para los procesos de continuidad del negocio.

[34] INSTITUTO POLITÉCNICO NACIONAL. Herramientas para hacking ético Simulación de intrusión Test de penetración pág. 5. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: <https://viclab.files.wordpress.com/2010/11/docfinal_pub.pdf>

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un software prototipo que brinde apoyo a las organizaciones que requieran implementar y parametrizar un SGSI basado en el gobierno de la seguridad de la información.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar las variables del gobierno de seguridad de la información basados en el manual de preparación al examen de CISM.

- Analizar los requerimientos de información que se necesitan para el establecimiento de un gobierno de seguridad de la información.

- Generar diagramas de casos de uso y flujogramas que permitan estructurar los procesos necesarios para establecer los flujos de entrada y salida de información en el software prototipo.

- Diseñar el modelo de base datos con el fin de estructurar las tablas, campos obligatorios, campos necesarios y consultas para facilitar el desarrollo del prototipo.

- Realizar el diseño y programación del prototipo.

- Realizar las pruebas del prototipo con el propósito de identificar las posibles fallas que se puedan presentar y realizar los ajustes necesarios para su estabilización y puesta en funcionamiento.

4. MARCO TEÓRICO

Se vive en un mundo tecnológicamente regido por redes sociales tecnologías de información, ciber ataques y amenazas a la seguridad de la información y a la disponibilidad de los recursos que la contienen. Las organizaciones ven con preocupación el sabotaje, fraude y robo, que en muchos casos se realizan por personas internas de la organización, por errores provocados por falta de controles adecuados o por procesos no definidos; todo esto causa en las organizaciones un impacto negativo representado en pérdidas financieras, multas, acciones legales, afectación sobre la imagen de la organización, estos problemas operativos afectan las estrategias de la organización y su correcto funcionamiento.[35]Las organizaciones no cuentan con un adecuado manejo de la seguridad de la información y no son lo suficientemente autodidactas para implementar modelos basados en estándares que proveen un adecuado manejo de la información y su seguridad, como base indispensable en la continuidad del negocio.[36]

Estos aspectos dejan ver que ya no basta con tener una protección a nivel de infraestructura, ni basta la adquisición de sistemas de seguridad como controles de acceso, detectores de intrusos cortafuegos entre muchos otros que pueden parecer suficientes para mantener seguro un sistema y a su información. Es por ello que es necesario adoptar soluciones que nos permitan proteger las fallas de seguridad que se puedan llegar a presentar. Estas soluciones no solo deben basarse en la infraestructura de seguridad, si no involucrar aspectos tales como un adecuado análisis de riesgos, asignación de roles y responsabilidades y marcos normativos.[37]

Al analizar todos estos aspectos en la seguridad de una organización los altos directivos se han dado cuenta que la información es un recurso critico si no el más importante de la empresa y por esto mismo debe tener un tratamiento adecuado como cualquier otro activo de la organización. La seguridad de la información se basa en la disponibilidad, integridad y confidencialidad de los activos de información.

La definición de roles y responsabilidad hace parte fundamental de un Gobierno adecuado de la seguridad de la información.

---

[35] ALTAMIRANO, Carlos. Modelo de Gobierno de seguridad de la información [Citado en: 21/06/2010][En línea], [consultado el 23 de octubre de 2016]. Disponible en: http://www.magazcitum.com.mx/?p=212#.VkudTdgvfIU

[36]Ibíd

[37]Ibíd

En este proceso se definen los grupos de trabajo y roles específicos para cumplir con las responsabilidades de seguridad de la información. de esta definición surgen las siguientes preguntas ¿quién hace qué?, ¿qué me toca? ¿Por qué a mí área? ¿Quién será el oficial de seguridad? ¿qué otros roles existen? ¿qué significa ser dueño de la información? ¿qué implica ser custodio de la información? Al responder a estas preguntas se asegura que se tiene una adecuada organización y distribución de las tareas roles y responsabilidades.[38]

El término gestión de los recursos se puede interpretar como:

La utilización adecuada del conocimiento y la infraestructura de seguridad de la información con eficacia eficiencia y efectividad. En el contexto de seguridad de la información la gestión de riesgos, es un proceso interactivo e iterativo para la evaluación y manejo de los riesgos y sus impactos, con el propósito de lograr los niveles de confidencialidad, integridad y disponibilidad óptimos para la organización, las preguntas que aquí se deben hacer corresponden a: ¿qué riesgos corre la información de nuestro negocio? ¿qué probabilidad existe de que se materialicen? ¿qué impacto tendrían en la operación? ¿se puede vivir con este riesgo? y si no: ¿qué se debe hacer para mitigarlo?,[39] al responder a estas preguntas se puede iniciar un proceso de identificación de los activos críticos de las organizaciones para su posterior análisis de riesgos, de allí que el software prototipo que se va a implementar para el proyecto de grado únicamente va a permitir recopilar en la base de datos los activos críticos de información mas no va a incluir el Análisis de riesgos de estos activos ya que este proceso es extenso aunque podría ser la continuidad o la creación de un módulo adicional al prototipo que se propone.

La Seguridad de la información debe estar regida por políticas, estándares, guías y procedimientos las cuales permiten tener un control de la operación del negocio. Lo importante es conocer cómo se debe cuidar la información y poder responder a los usuarios cuando preguntan ¿para qué sirve que cambie mi contraseña cada 3 meses? ¿por qué debo bloquear mi máquina cuando abandono mi lugar? ¿Qué pasa si comparto mi contraseña, aunque sea “por un día”? Así mismo la normatividad dictará qué pasa si alguien no se alinea con las políticas, que consecuencias se podrían llegar a presentar y cuáles serían los lineamientos a seguir en esos casos.[40]

Establecer y monitorear los indicadores de cumplimiento de los objetivos de seguridad, el porcentaje de áreas de negocio que han realizado análisis de riesgos de seguridad en el año, el nivel de vulnerabilidad de los sistemas críticos de

[38] ALTAMIRANO, J.C. Io. Cit, p. 17
[39] Ibód.
[40] Ibíd.

información, el porcentaje de empleados con responsabilidades de seguridad que ya han recibido un entrenamiento formal en seguridad de la información, la capacidad de respuesta a incidentes, hace parte fundamental de la medición de los resultados de los procesos y procedimientos adoptados en la seguridad de la información. Es por esta razón que en esta actividad de medición se debe responder a la pregunta ¿sabemos que se están haciendo bien las cosas?[41]

Dentro de los beneficios que se observan acerca de una adecuada administración del gobierno de seguridad en una organización podrían ser:

La toma de decisiones acertadas en materia de seguridad gracias a la información actualizada de lo que está pasando: los riesgos, los avances, indicadores de seguridad, la reacción oportuna y ágil ante incidentes de seguridad gracias a la clara definición de roles y responsabilidades, disminuyendo los impactos que se puedan llegan a presentar.42Mayor conciencia de la gente dentro y fuera de la organización sobre la importancia de la seguridad, ayudando a prevenir fugas de información por ataques de ingeniería social[43]. Aumento en el grado de confianza de los clientes y socios de las organizaciones al asegurar que la información se encuentra manejada por un modelo de gobierno que permanentemente vigila y mitiga los riesgos. Disminución de los riesgos relacionados con la confidencialidad, integridad y disponibilidad de la información.[44]

Otro de los temas importantes

En cuanto a seguridad de la información contemplan: los procesos y normatividad que deben ser adoptadas por las organizaciones en pro de evitarse problemas jurídicos y de legalidad, algunas de las normas vigentes en el marco colombiano incluyen temas como derechos de Autor, propiedad industrial, propiedad intelectual, comercio electrónico y firmas digitales, decreto 2364 de 2012 – firma electrónica, decreto 2609 de 2012 – expediente electrónico, decreto 2693 de 2012 – gobierno electrónico, decreto 1377 de 2013 – protección de datos personales, decreto 1510 de 2013 – contratación pública electrónica, decreto 333 de 2014 – entidades de certificación digital, suplantación de identidad (apropiación del nombre, contraseñas y/o patrimonio de otra persona con el propósito de realizar actos delictivos.)45 , alteración de la información, ausencia de Disponibilidad,

[41] ALTAMIRANO, J.C.Op. Cit. p. 18
[42] CÁMARA VENEZOLANA DE EMPRESAS DE TECNOLOGÍAS DE INFORMACIÓN Gobernabilidad y seguridad de la información beneficios. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: http://www.cavedatos.net/eventos/?i=65>
[43]ALTAMIRANO, Op. Cit. p. 19
[44] Ibíd.
[45]INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA. Suplantación de identidad. . [En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://www.incibe.es/search/ ?allSearch Field=suplantar identidad>

ausencia de Confidencialidad, autenticidad, Integridad, no repudio (negar un mensaje transmitido por un receptor o emisor).[46]

5. DISEÑO METODOLÓGICO

Este proyecto se enmarca metodológicamente como proyecto de desarrollo tecnológico obteniendo como resultado un activo representado en un software prototipo que brinde apoyo a las organizaciones para implementar y parametrizar un SGSI basado en el gobierno de la seguridad de la información.

Analizando las variables que intervienen en el Gobierno de seguridad, hemos establecido unas directrices para estructurar el software prototipo basado en el gobierno de seguridad estándar para cualquier tipo de empresa y las normas internacionales ISO 27001:2013[47]- 27014 así como la proveniente de ISACA[48] en el dominio de Gobierno de Seguridad de la información.

Uno de los objetivos específicos para la propuesta de tesis es la de realizar el proceso de análisis de los requerimientos, diseño y programación del prototipo en lenguajes de programación orientada a objetos. Se propone para recopilar la información de forma ágil y organizada utilizar bases de datos en SQL server 2014 a su vez Diseñar una interfaz amigable utilizando herramientas de desarrollo de software que se ajusten a los requerimientos del prototipo para este fin se programara en .net framework 4.0 lenguaje c#.

Se ha pensado trabajar de manera modular el software prototipo de forma conjunta con las diferentes áreas que componen la estructura organizacional de una empresa involucrando a personas, procesos y recursos.

Se sabe que el personal de la empresa tiene definidas sus funciones y conoce de antemano con qué recursos cuenta para poder realizar su trabajo diariamente, es por esto que a través de las personas se podrá recolectar la información ágilmente con eficiencia eficacia y efectividad obteniendo información actualizada y veraz que le permitirá al oficial de seguridad poder analizar la información y tomar decisiones acertadas para proponer mejoras en la seguridad de la información o para establecer un gobierno de seguridad de la información que involucre todas

[46]ARCHIVO GENERAL DE LA NACIÓN, Compilación normativa 2014. . [En línea], [consultado el 23 de octubre de 2016]. Disponible en: <http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/SINAE/Productos%20SINAE%202013/Compilacion_Normativa.pdf>

[47]INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Sistema de Gestión de la Seguridad de la Información. ISO/IEC 27001:2013. Bogotá D.C. 2013

[48]ISACA. Manual de Preparación al Examen CISM 2014.Impreso en Estados Unidos de América. ISBN 978-1-60420-410-0

aquellas responsabilidades y prácticas que ejerce y aprueba la alta dirección de una empresa en cuanto a la seguridad de la información.

5.1 IDENTIFICACIÓN DE LAS VARIABLES DEL GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN

En la mayoría de las organizaciones se ha constituido un gobierno corporativo constituido por accionistas, junta directiva y la alta administración sin embargo, se ha obviado una rama del gobierno representado en el gobierno de seguridad de la información el cual se ha tenido que ir incorporando a medida que se ve la necesidad de responder acerca de las regulaciones legales y civiles en las empresas.[49]

Un gobierno de seguridad efectivo debe tener en cuenta seis resultados básicos entre los cuales se pueden mencionar[50]

5.1.1 Alineación estratégica. Alinear la seguridad de la información con la estrategia de negocio para apoyar los objetivos organizacionales.

5.1.2 Gestión de riesgos. Permite gestionar un inventario de activos para el análisis del riesgo con el fin de ejecutar medidas apropiadas para mitigar los riesgos y reducir el impacto ante una vulnerabilidad y amenaza de la organización.

5.1.3 Entrega de valor. Permite optimizar la inversión en seguridad en apoyo a los objetivos del gobierno corporativo.

5.1.4 Optimización de recursos. Desarrollar arquitecturas de seguridad para definir y utilizar los recursos de la infraestructura tecnológica de manera eficiente.

5.1.5 Medición de desempeño. Monitorear los procesos de seguridad de la información implementados

5.1.6 Integración. Integrar todos los factores críticos para la organización o empresa con el fin de asegurar los procesos de la gestión de seguridad de la información.

---

[49] ISACA. Manual de Preparación al Examen CISM 2014.Impreso en Estados Unidos de América. ISBN 978-1-60420-410-0

[50] Ibíd

Una vez que los Directivos o accionistas han llegado a entender los beneficios significativos al incorporar un gobierno de la seguridad de la información ven la necesidad de:[51]

- Tener cuidado para proteger el debido cumplimiento regulatorio.

- Reducir el riesgo a niveles definibles y aceptables

- Optimizar las asignaciones de los limitados recursos de seguridad

- Fortalecer el nivel de certeza en las decisiones críticas para que no se basen en información imprecisa

- Proporcionar información sólida para la gestión de riesgo eficiente y efectivo para mejorar los procesos de la gestión de incidentes y de continuidad del negocio.

- Mejorar la confianza en las relaciones con los clientes

- Proteger la reputación de la organización

- Mejorar las transacciones electrónicas de la empresa u organización

- Teniendo en cuenta la información adquirida por la empresa u organización como son las políticas del gobierno corporativo, el objetivo general y los objetivos específicos se tiene una línea base para:

- Una estrategia integral de seguridad de la información que se integra con el objetivo de la empresa u organización.

- Se crean proponen políticas de gobierno de seguridad las cuales deberán ser puestas en aprobación por los altos directivos de la organización para que sean de obligatorio cumplimiento.

- Se crean estándares para cada política de seguridad.

- Se propone una estructura organizacional para la empresa u organización donde se incluya el gobierno de seguridad de la información donde se tenga una autoridad libre de conflictos y recursos adecuados.

[51]Ibíd-

- Métricas y procesos de monitoreo para el gobierno de seguridad propuesto.

- Implementar auditorías internas a intervalos planificados con el fin de medir si el gobierno de la seguridad de la información va acorde a los propios requisitos de la organización o empresa y estén alineados a la norma ISO IEC 27001:2013

- Generar una gestión de riesgo una vez obtenida el inventario de activos que sean críticos para la Empresa u Organización.

- Generar planes de capacitación, concienciación y formación en seguridad de la información al personal

- Generar planes de mejora y tomar acciones correctivas para resolver cualquier deficiencia en seguridad de la información.

- Entrega de reportes a la alta dirección con el fin de asegurar la efectividad y eficiencia de todo el sistema de gobierno de seguridad de la información, entre los reportes están: inventario de activos de información con una tentativa en la clasificación y valoración, revisión periódica a la alineación de los objetivos del negocio críticos con los objetivos del gobierno de seguridad de la información.

5.2 ANÁLISIS DE LOS REQUERIMIENTOS DE INFORMACIÓN PARA ESTABLECER UN GOBIERNO DE SEGURIDAD

Basados en el Manual de Preparación al Examen CISM de ISACA en el dominio del Gobierno de seguridad de la información y en las variables identificadas se analizan los requerimientos de información necesarios que deben tener los formularios de la aplicación asi:

5.2.1 Contexto Empresarial. En este formulario se solicitará información básica de la empresa se podrá incluir el logo corporativo, nombre de la empresa, seleccionar la actividad económica de una lista desplegable con información actualizada de la cámara de comercio, ingresar el nit de la empresa, el año de creación de la empresa con él se podrá llegar a obtener un acercamiento sobre el nivel de madurez de la empresa en cuanto a sus procesos. datos misionales (misión visión y objetivos), Así mismo se indagará acerca de las políticas empresariales que se tienen en seguridad de la información. Datos que serán indispensables para las siguientes fases de identificación y clasificación de los activos estratégicos de información de la empresa, siendo estos la base fundamental del software prototipo planteado.

- Nombre de la empresa
- Actividad Económica
- Nit
- Año de creación de la empresa
- Misión
- Visión
- Objetivo general
- Políticas empresariales en seguridad de la información.

5.2.2 Análisis DOFA. Una vez recolectada la información de la empresa, se realiza un análisis DOFA en seguridad de la información, este análisis va a permitir identificar los problemas Internos y externos de la organización, las debilidades, las fortalezas y las oportunidades, de esta forma se llegaría a tener un esquema preliminar de una gestión de riesgo que al sumarla al inventario de activos de información podria mostrar una perspectiva general sobre el proceder de los cumplimientos legales y una posible afectación económica.

5.2.2.1 Fortalezas. Las empresas deben evaluar los puntos fuertes de su sistema de información. Esto incluye temas como la evaluación de la eficacia de los cortafuegos, configuración/ajustes de contraseña y protocolos de transferencia de información. Muchos programas de productividad en el lugar de trabajo "off theshelf" (fuera de la plataforma) tales como Microsoft Office e Internet Explorer vienen con una función de protección de seguridad. Sin embargo, las grandes empresas con múltiples ubicaciones a menudo tienen que ir mucho más allá de las soluciones "off theshelf" (fuera de la plataforma).[52]

5.2.2.2 Debilidades. Las empresas deben evaluar con realismo las debilidades de sus sistemas de seguridad de IT. Las debilidades típicas se presentan en forma de violaciones de seguridad de los empleados, robo de los empleados y protocolos de transferencia de información defectuosos. Incluso la falta de fondos puede ser una debilidad porque las empresas no tienen el capital operativo necesario para solucionar correctamente una vez que las principales debilidades sean detectadas.[53]

[52] DWIGHT CHESTNUT. Análisis FODA de Seguridad, [En línea], [consultado el 23 de octubre de 2016]. Disponible en: www.ehowenespanol.com/analisis-foda-seguridad-sobre_145898//
[53] Ibíd.

5.2.2.3 Oportunidades. Representadas en las opciones que el mercado ofrece para la seguridad de la información, leyes, normas, capacitaciones, tecnologías, servicios entre otros.

5.2.2.4 Amenazas. Ataques de seguridad que se originan fuera de la empresa. El ejemplo más común es un ataque de un pirata o un virus informático distribuido masivamente.[54]

5.3 ANÁLISIS POR PROCESOS

Teniendo como base los objetivos misionales del negocio se propone realizar el levantamiento de la información a niveles de objetivos por cada área de la empresa para ello se debe analizar la información que se maneja por áreas, así como los procesos misionales que maneja la organización, las personas involucradas en los procesos y los recursos que utilizan para su labor diaria, información que será ingresada al sistema por las personas que hacen parte del equipo de trabajo de cada área de la empresa, de esta forma se podrán identificar los roles, responsabilidades y recursos utilizados para cumplir los objetivos del área alineados con los objetivos misionales de la empresa. Así mismo se propondrán encuestas orientadas a un ambiente de seguridad de información dentro de sus áreas de trabajo y a nivel empresarial las cuales pueden permitirla identificación de huecos de seguridad y o vulnerabilidades en las diferentes áreas o procesos.

5.4 IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN CRÍTICOS.

Se obtendrá de cada área de la organización la descripción de los activos de información que son críticos para cada proceso, describiendo el tipo de activo, así como todas las acciones o medidas necesarias para garantizar el cumplimiento de sus objetivos, entre los que se deben encontrar la seguridad de la información entre otros, determinado a través de la información suministrada las propuestas de una clasificación y valores de los mismos, con el fin de determinar para la organización un análisis de riesgo preliminar identificando los atributos que se debe tener en cuenta para la protección del activo de información.

Con la información recolectada en el contexto empresarial, el análisis de los procesos y la evaluación de los activos a niveles de confidencialidad, integridad y disponibilidad se llega a identificar cuales activos son críticos para la organización

[54] Ibíd.

y cuales necesitan un nivel de seguridad más estricto. Así mismo la certificación de NTC-ISO9001 en calidad y gestión de calidad que ha sido implementada en algunas organizaciones permitirá obtener un detalle más preciso de los activos de información que intervienen en los procesos críticos de las empresas y a su vez identificar los riesgos que pueden causar perdida del objetivo misional de la estrategia de la organización. No obstante, es importante realizar una clasificación de la información en pública, privada, semiprivada, confidencial y especificar los medios de almacenamiento de dicha información, asignar roles y responsables de la misma y los recursos utilizados para su resguardo y tratamiento.

5.5 OBJETIVOS DE SEGURIDAD

Una vez se establezcan cuáles son los objetivos de negocio se propone el establecimiento de los objetivos de seguridad los cuales deben estar alineados estratégicamente con los objetivos del negocio basándose en las normas regulatorias a niveles de seguridad y marcos legales. Cuatro ítems son de vital importancia para plantear los objetivos de seguridad[55] **Organización** (Matriz RACI) Roles y responsabilidades a nivel de seguridad de la información, **planes** (Acciones, responsables, administración adecuada de recursos), **políticas** de seguridad teniendo en cuenta la norma **ISO 27001:2013**, **metas** a niveles de madurez en seguridad de la información.[56]

Para el establecimiento d**e las políticas** se toma un modelo estándar basado en la norma ISO 27001:2013 así:

- Política de Seguridad de la Información
- Política de la Organización de la Seguridad de la Información
- Política de Continuidad de Negocio
- Política de Seguridad Física y del Entorno
- Política de los Recursos Humanos
- Política de Gestión de Activos
- Política de Control de Acceso
- Política de Seguridad de Operaciones
- Política Seguridad de las Comunicaciones
- Política de Transferencia de Información
- Política Relaciones con los Proveedores
- Política de Gestión de Incidentes de Seguridad de la Información

[55] ISACA. Op. Cit. p. 26
[56] Ibíd.

- Política de Cumplimiento.

5.6 PLANES DE SEGURIDAD

Por último, se plantean los flujos de procesos por áreas y los planes de seguridad, estos últimos nos permiten identificar los responsables de la seguridad en la organización, las acciones que se deben llevar a cabo para que se cumplan los objetivos de seguridad estipulados, los recursos utilizados para su establecimiento y los tiempos en los cuales se deben llevar a cabo todas las labores para el establecimiento de la seguridad de la información en la empresa.

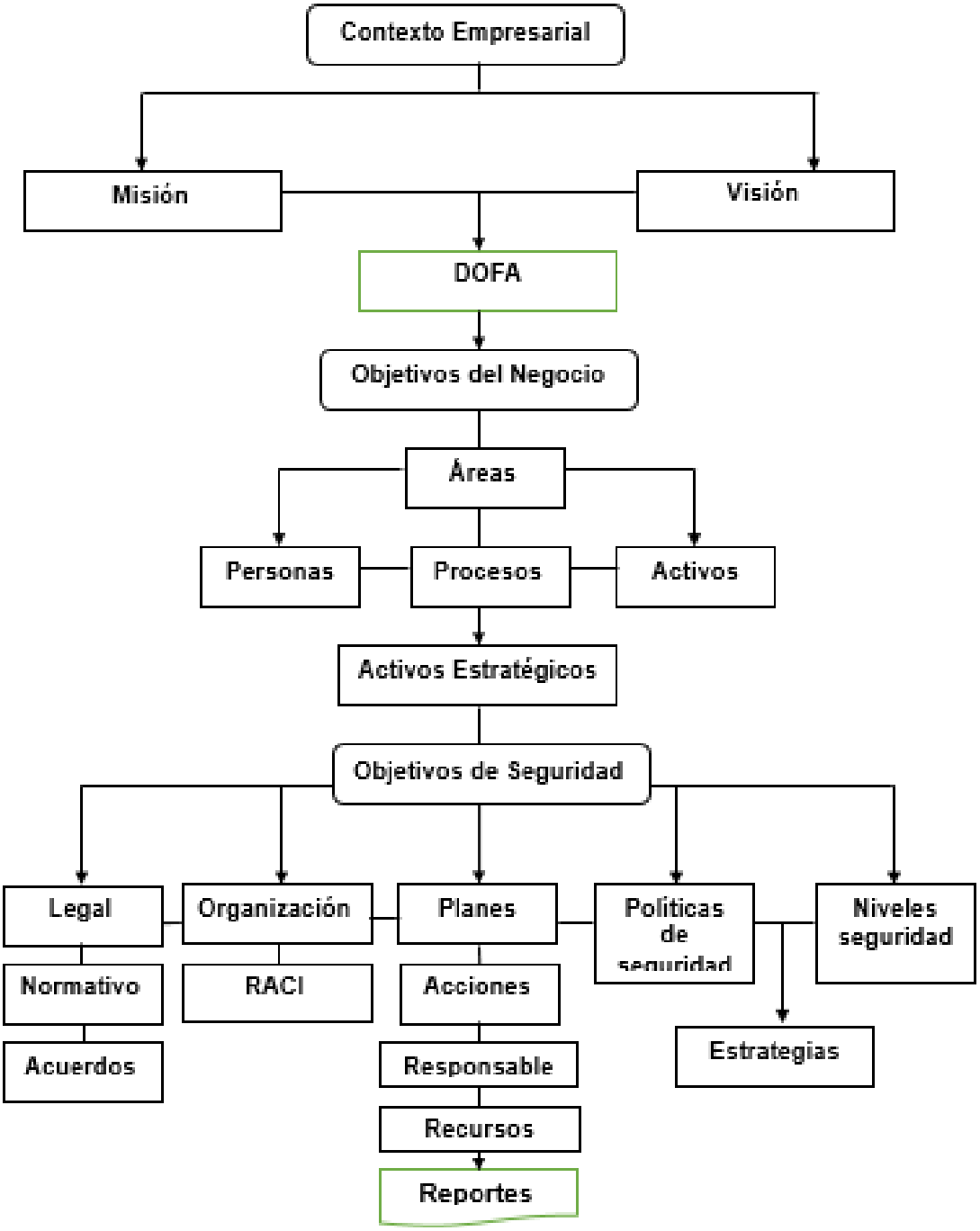
6. DIAGRAMA DE FLUJO Y CASOS DE USO

Tomando los conocimientos de la norma ISO 27001-2013 e ISACA en el dominio del gobierno de seguridad de información se ve la necesidad de crear un diagrama de flujo que facilite la organización lógica de los pasos a seguir y que sirva en el proceso de desarrollo del prototipo. Con base en el diagrama de flujo propuesto, se plantean los diferentes casos de uso que permitirán observar la interacción de las personas con el sistema. En este capitulo se podrá observar el diagrama de flujo propuesto, así como los diferentes diagramas de casos de uso utilizados para el desarrollo del prototipo.

6.1 DIAGRAMA DE FLUJO El diagrama de flujo propuesto en la figura1, muestra los pasos lógicos que debe seguir el desarrollo del prototipo, como son: el Contexto empresarial (misión visión, objetivos y políticas de seguridad; los objetivos de negocio: áreas, procesos, personas y activos de información, asi como en los niveles de confidencialidad, integridad y disponibilidad que deben tener los activos; el resultado de este análisis se representa en la identificación de los activos críticos de información que según el estándar Magerit[57] se puede representar en: activo de información, software, hardware, red, equipamiento auxiliar, instalación, servicios y personal. Los objetivos de seguridad están representados a niveles Legal, Normativo, Acuerdos, organización (matriz Raci) roles y responsabilidades en seguridad de la información, planes, acciones, y recursos orientados a la seguridad de la información, políticas de seguridad, estrategias orientadas al establecimiento de la seguridad de la información. Por último, se pueden encontrar los reportes, estos son indispensables para el oficial de seguridad en su proceso de análisis y son los que permitirán a los altos directivos tomar adecuadas y acertadas decisiones misionales orientadas al establecimiento de la seguridad de la información en sus procesos, activos y así evitar acciones legales.

[57] http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/321_paso_1_inventario_de_activos.html

Figura 1. Diagrama de flujo gobierno de seguridad de la información



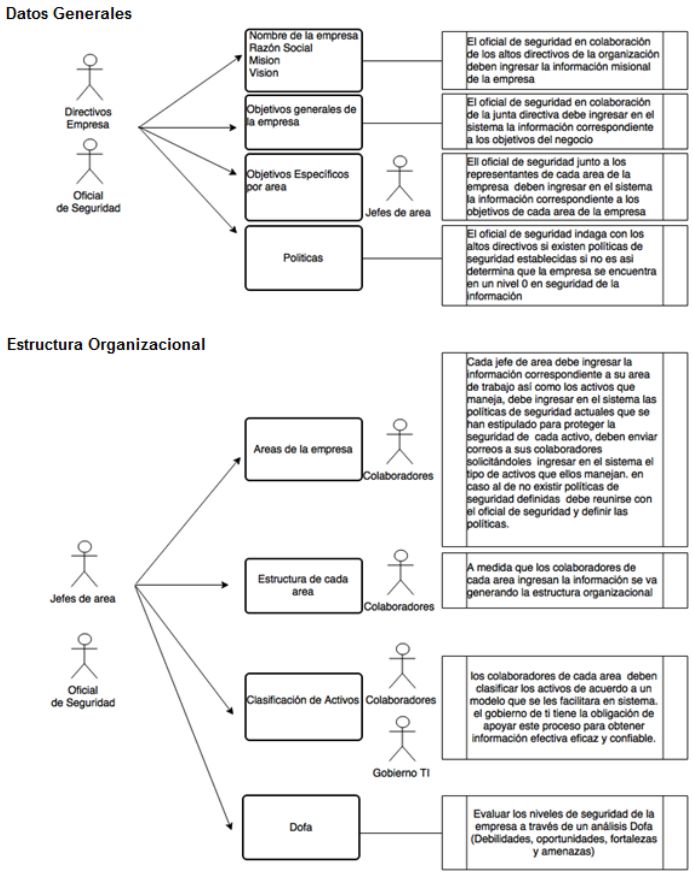
Fuente. Autores

6.2 CASOS DE USO

Los diagramas de casos de uso se plantean en el diseño del prototipo ya que son una estructura que ayuda y permitirá determinar la forma en la cual se va a usar el prototipo y las personas o actores que van a hacer uso del mismo. A continuación se realizara una descripción de los casos de uso propuestos.

6.2.1 Datos generales y estructura organizacional. En la figura 2 se puede ver gráficamente la representación de los casos de uso de como se capturan los datos generales de la empresa y su estructura organizacional, en ellos se puede observar la interacción de las personas como el oficial de seguridad, directivos y jefes de área con el sistema.

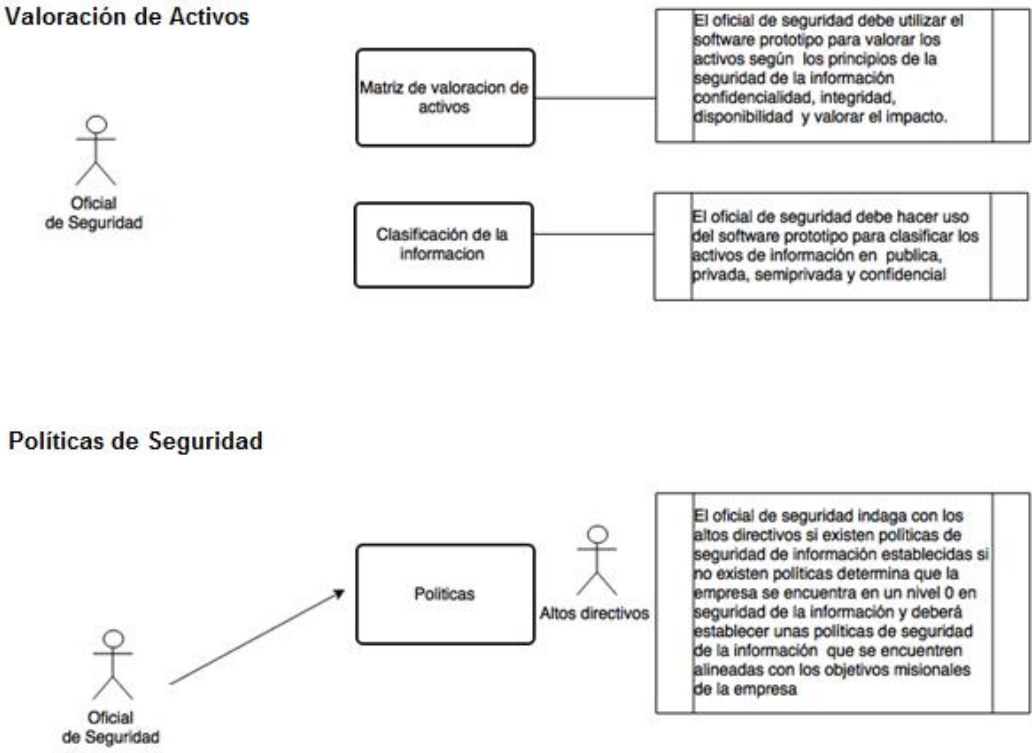
Figura 2. Datos generales y estructura organizacional



Fuente. Autores

6.2.2 Valoración de activos de información y políticas de seguridad. En la figura 3 se puede ver gráficamente la representación de los casos de uso en los cuales el oficial de seguridad realiza la valoración de los activos de información y junto con el grupo directivo genera una política de seguridad orientada a la protección de la información.

Figura 3. Casos de uso valoración de activos y políticas de seguridad



Fuente. Autores

6.2.3 CASOS DE USO UML. A continuación se muestra una descripción extendida de los casos de uso propuestos en el diseño del prototipo.

6.2.3.1 Ingresar datos generales. En el cuadro 1 se muestra como debe ser el ingreso de la información de la empresa como el nombre de la empresa, actividad económica de la empresa, año de creación de la empresa, misión, visión, objetivos, políticas definidas en la empresa que estén orientadas a la seguridad de la información.

Cuadro 1. Caso de uso ingresar datos generales

CU-01	**Ingresar Datos Generales**	
Versión	1.0(03/08/2016)	
Dependencias	D01 Ingresar los datos de la empresa (Nombre,) D02 Ingresar la información misional (misión, visión) D03 Objetivos D04 Políticas de seguridad	
Precondición	La empresa y altos directivos facilitaran los medios necesarios para obtener la información solicitada para realizar el Ingreso de los datos y objetivos misionales del negocio.	
Descripción	Aquí se debe ingresar los datos generales de una empresa.	
Secuencia Normal	**Paso** 1	**Acción** Logo Nombre empresa Actividad económica Nit Año Creación de la empresa Numero empleados Misión Visión Objetivo General Política de Seguridad
Comentarios	Es importante la participación de la alta gerencia y los jefes de departamentos, así como la participación activa del personal administrativo de la empresa en cada proceso de recolección de información.	

Fuente: Autores

6.2.3.2 Caso de uso análisis Dofa. En este caso de uso se propone el ingreso de la información correspondiente al dofa de la empresa representado en las oportunidades externas que pueden ser adoptadas por la organización para mejorar en la seguridad de la información, la identificación de las amenazas externas a las cuales se expone la organización, identificación de las vulnerabilidades o fallos internos de seguridad en la empresa, identificación de las debilidades que la empresa presenta en seguridad de la información, estrategias identificadas en fortalezas-amenazas,fortalezas-oportunidades,debilidades-amenazas, debilidades-oportunidades. tal como se puede observar en el cuadro 2 a continuación.

Cuadro 2. Caso de uso análisis DOFA en seguridad de la información

CU-02	**Análisis Dofa en seguridad de la información**	
Versión	1.0(03/08/2016)	
Dependencias	F01 Ingresar Oportunidades F02 Ingresar Debilidades F03 Ingresar Amenazas F04 Ingresar Fortalezas	
Precondición	La empresa y altos directivos facilitaran los medios necesarios para obtener la información solicitada para realizar el Ingreso de los datos solicitados por el sistema.	
Descripción	Aquí se debe ingresar las oportunidades externas que pueden ser adoptadas por la organización para mejorar en la seguridad de la información, identificar las amenazas externas a las cuales se expone la organización, identificar las vulnerabilidades o fallos internos de seguridad de la empresa, identificar las debilidades que la empresa presenta en seguridad de la información, a su vez deberá proporcionar 4 estrategias identificadas así: Fortalezas-Amenaza, Fortalezas-Oportunidades, Debilidades-Amenazas, Debilidades-Oportunidades	
Secuencia Normal	**Paso** 1	**Acción** Fortalezas, oportunidades, amenazas, debilidades, estrategia, fortalezas, amenazas.
Comentarios	Es importante la participación de la alta gerencia y los jefes de departamentos, así como la participación activa del personal administrativo de la empresa en cada proceso de recolección de información.	

Fuente: Autores

6.2.3.3 Caso de uso objetivos de negocio. En este caso de uso se plantea recopilar la información correspondiente a las áreas de la empresa, los procesos, las personas, los recursos y la información, tal como esta descrito en el cuadro 3.

Cuadro 3. Caso de uso Objetivos de negocio

CU-03	**Objetivos de negocio**	
Versión	1.0(03/08/2016)	
Dependencias	E01 Ingresar los datos de las áreas que conforman la estructura organizacional de la empresa. E02 Objetivos Generales del área. E04 Objetivos identificados en los procesos que están a cargo del área	
Precondición	Colaboración de los jefes de área y personal a su cargo para realizar la recopilación e ingreso de la información de cada área que conforma la estructura organizacional de la empresa.	
Descripción	Este caso de uso recopilara la información de las áreas de la empresa los procesos los procesos, personas, recursos e información	
Secuencia Normal	**Paso 1**	**Acción** Ingresar la información áreas que conforman la estructura organizacional de la empresa Nombre del Área Misión Visión del área Objetivos del área Nombre integrantes del área Cargos que ocupan dentro del área Políticas de seguridad en el área Nombre de los procesos por prioridad
Comentarios	Es importante la participación de la alta gerencia, los jefes de departamentos, personal de la empresa en cada proceso de recolección de información.	

Fuente: Autores

6.2.3.4 Caso de uso valoración de activos estratégicos. En el cuadro 4 se observa que para realizar la identificación de los activos críticos de la empresa se debe iniciar valorando en los activos los niveles de confidencialidad, integridad y disponibilidad, asi como la alineación estratégica, las políticas y los objetivos misionales de la empresa entre otros. Se organiza la información en pública, privada, semiprivada, confidencial y se especifican los medios de almacenamiento, se asignan roles y responsables de la información.

Cuadro 4. Caso de uso valoración de activos estratégicos

CU-04	**Valoración de Activos estratégicos**	
Versión	1.0(03/08/2016)	
Dependencias	A01seleccionar los activos de la empresa que hacen parte de los procesos estratégicos alineados con los objetivos misionales de la organización. A02 Ingresar la información de las personas que custodian, son propietarias o usuarias de los activos A03 Clasificar e identificar los activos representados en software, hardware, información, red, servicios, instalaciones, personal, e intangibles y determinar los grados de Confidencialidad, Disponibilidad e integridad de los mismos. A04 Valorar los activos críticos de la empresa	
Precondición	Obtener la colaboración de todas las áreas o procesos y personal de la empresa, así mismo contar con la participación de los altos directivos y jefes de área para poder identificar los activos de información críticos de la empresa. Contar con el apoyo del área de tecnología para poder obtener la lista de activos tecnológicos asignados a las diferentes áreas de la organización. Recibir los documentos políticas y controles de seguridad estipuladas por el departamento de TI para el manejo adecuado de los recursos y activos de la empresa.	
Descripción	Identificación de los activos de la empresa, su importancia representada en los principios de la seguridad de la información como la confidencialidad, integridad y disponibilidad, se debe tener presente la alineación estratégica entre los activos políticas y objetivos misionales de la empresa con el fin de asegurar que las decisiones no se basen en información defectuosa o desactualizada. De tal forma se obtendrá un resumen detallado de los activos de información y obtener el tipo de clasificación de la información que la organización maneja como puede ser pública, privada, semiprivada, confidencial asi mismo especificar los medios de almacenamiento de dicha información asignar roles y responsables de la información.	
Secuencia Normal	**Paso**	**Acción**
	1	Identificación de procesos críticos e identificación de activos estratégicos de información.
	2	Ingresar la información de los activos de la organización representados en: Información, software, físicos, servicios, personas, intangibles.
	3	Identificar en los activos críticos los grados de: Confidencialidad Integridad Disponibilidad Basados en el costo de recuperación
	4	Identificar el tipo de información dependiendo de su naturaleza e importancia. Confidencial Personal Privada Semiprivada
Condiciones	Es importante la participación de la alta gerencia, los jefes de departamentos, personal de la empresa y en especial el departamento de Tecnología. Recolección de información.	

Fuente: Autores

6.2.3.5 Caso de uso objetivos de seguridad. El cuadro 5 muestra cómo se recopilara la información que corresponde a los roles y responsabilidades adquiridos en pro de establecer un gobierno de seguridad de la información, así como los planes, políticas y normatividad.

Cuadro 5. Caso de uso objetivos de seguridad de la información

CU-05	**Objetivos de seguridad de la información**	
Versión	1.0(03/08/2016)	
Dependencias	S01 Legal, Normativo, Acuerdos S02 Organización (matriz Raci) Roles y Responsabilidades en seguridad de la información S03 Planes, Acciones, Recursos orientados a la seguridad de la información S04 Políticas de seguridad S05 Estrategias orientadas al establecimiento de la seguridad de la información.	
Precondición	Colaboración de los jefes de área y personal a su cargo para realizar la recopilación e ingreso de la información de cada área que conforma la estructura organizacional de la empresa.	
Descripción	Este caso de uso recopilara la información que corresponde a los roles y responsabilidades adquiridos en pro de establecer un gobierno de seguridad de la información, asi como los planes, políticas y normatividad.	
Secuencia Normal	**Paso 1**	**Acción** RACI Planes (Acciones, responsables, recursos) Políticas Marco legal, normativo, acuerdos cliente
Excepciones	**Paso**	**Acción**
Comentarios	Es importante la participación de la alta gerencia, los jefes de departamentos, personal de la empresa en cada proceso de recolección de información.	

Fuente: Autores

6.2.3.6 Caso de uso políticas de seguridad. El cuadro 6 muestra cómo se llevará a cabo la captura de la información que corresponde a la definición de las políticas de seguridad en pro de establecer un gobierno de seguridad de la información.

Cuadro 6. Caso de uso políticas de seguridad

CU-06	**Políticas de Seguridad**	
Versión	1.0(03/08/2016)	
Dependencias	P01 Identificar las políticas empresariales P02 Identificar las políticas empresariales de cada área de la organización para los activos asignados P03 Proponer políticas de seguridad de la información basada en información real de procesos, personal y recursos. P04 Identificar la legislación que aplica a la organización basada en la criticidad y protección de sus activos para de esta manera evitarle a la empresa multas y acciones legales.	
Precondición	Obtener la colaboración de la alta gerencia para el establecimiento de políticas de seguridad y actualización de las ya existentes. Contar con la participación activa de los líderes de las diferentes áreas de la empresa. Recibir apoyo y colaboración del departamento de tecnología para poder establecer políticas acordes con los hallazgos encontrados en el análisis de los activos. Asimismo coordinar y supervisar la correcta operación y funcionamiento de la infraestructura, y servicios tecnológicos de la organización.	
Descripción	se utilizarán formatos preestablecidos para agilizar el proceso de creación de políticas de seguridad se dará la opción de modificación a las políticas para alinearlas con la estrategia de la organización en este caso como la propuesta es un prototipo se generará una platilla estándar sobre la cual nos basaremos por cada tipo de activo. Además, se generarán plantillas que permitirán capacitar a los empleados en seguridad de la información.	
Secuencia Normal	**Paso** **1** **2** **3**	**Acción** Analizar las políticas establecidas por la empresa Analizar las políticas establecidas por el área de tecnología en la protección de sus recursos. Proponer nuevas políticas de seguridad de la información basadas en los hallazgos hechos con el análisis realizado a los activos críticos de la organización y alinearlas según los objetivos misionales de la organización
Comentarios	Es importante la participación de la alta gerencia, los jefes de departamentos, personal de la empresa y en especial el departo de Tecnología de la empresa en cada proceso de recolección de información.	

Fuente: Autores

6.2.3.7 Caso de uso estrategias de la seguridad de la información. En el cuadro 7, se muestra el proceso que se llevará a cabo para definir las estratégias de seguridad de la información.

Cuadro 7. Caso de uso estrategias de la seguridad de la información

CU-07	**Estrategias de la seguridad de la información**	
Versión	1.0(03/08/2016)	
Precondición	Colaboración de los jefes de área y personal a su cargo para realizar la recopilación e ingreso de la información de cada área que conforma la estructura organizacional de la empresa.	
Descripción	La estrategia debe ser establecida por la organización y definida por los atributos de negocio y de seguridad de la información.	
Secuencia Normal	Paso 1	Acción Un objetivo: lo que se busca alcanzar a través de la ejecución de la estrategia. Acciones: actividades a ejecutar para cumplir con lo definido en la estrategia. Resultados: lo que se espera obtener de esas acciones que permiten cumplir con el objetivo propuesto. Tiempos: periodo en el cual se debe ejecutar la estrategia. Métricas: mecanismos para monitoreo y seguimiento a la implementación e impacto en las diferentes instituciones. Seguridad de la información según el dominio del gobierno de seguridad ISACA
Comentarios	Es importante la participación de la alta gerencia, los jefes de departamentos, personal de la empresa en cada proceso de recolección de información.	

Fuente: Autores

6.2.3.8 Caso de uso informes. El cuadro 8 representa la definición de los informes que el sistema mostrará basado en la información recolectada a travez de los módulos del prototipo en pro de establecer un gobierno de seguridad de la información.

Cuadro 8. Caso de uso informes

CU-08	**Informes**	
Versión	1.0(03/08/2016)	
Dependencias	I01Ingreso completo de la información solicitada en cada módulo del software.	
Precondición	Colaboración de los jefes de departamentos y personal a su cargo para realizar la recopilación e ingreso de la información completa de cada área que conforma la estructura organizacional de la empresa. Si no se llegara a tener completa esta información los informes y reportes generados por el software propuesto no tendrían los resultados esperados.	
Descripción	Generación de reportes y documentos indispensables en el establecimiento de un Gobierno de seguridad de la información basados en la recopilación de los datos obtenidos a través del software propuesto.	
Secuencia Normal	**Paso**	**Acción**
	1	Una vez obtenida la información completa de cada módulo del software se generan los correspondientes reportes.
Comentarios	Es importante la participación de la alta gerencia, los jefes de departamentos, personal de la empresa en cada proceso de recolección de información.	

Fuente: Autores

7. MODELO ENTIDAD RELACIÓN BASE DE DATOS

El primer paso en el diseño de una base de datos relacional es la creación de la base datos, la configuración de cada una de las tablas (Entidades), la programación de los procedimientos almacenados (create, read, update, delete) y el establecimiento de las claves primarias y foráneas de las entidades. Por último la identificación de las relaciones entre las entidades a través de sus llaves. A continuación, se describirán las entidades creadas en el desarrollo del proyecto y se enumerarán los procedimientos almacenados programados de acuerdo a las especificaciones funcionales que el software demanda.

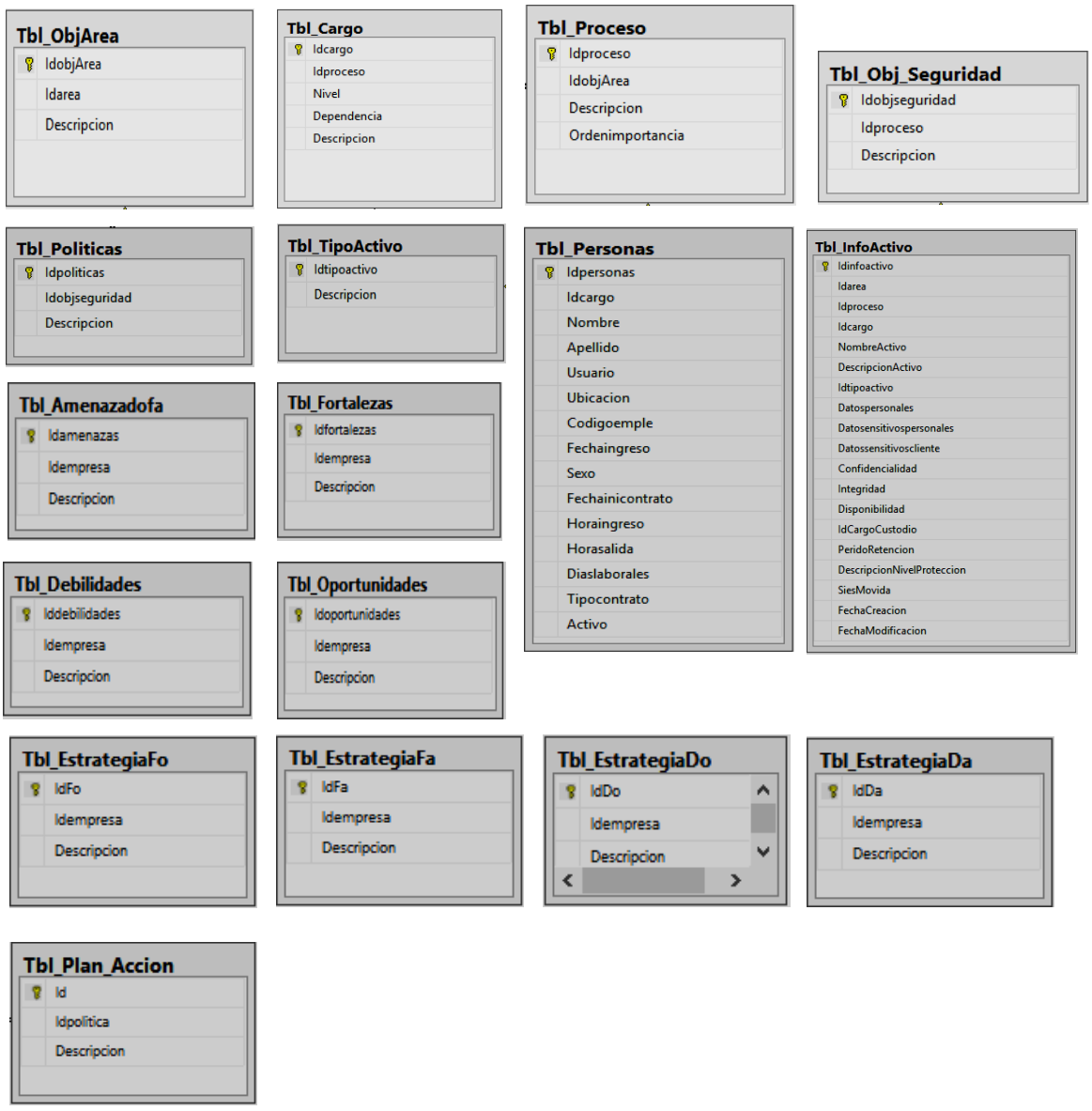
7.1 ENTIDADES

Un objeto no es más que un conjunto de variables (o datos) y métodos (o funciones) relacionados entre sí. Los objetos en programación se usan para modelar objetos o entidades del mundo real . Un objeto es, por tanto, la representación en un programa de un concepto, y contiene toda la información necesaria para abstraerlo: datos que describen sus atributos y operaciones que pueden realizarse sobre los mismos.[58] La figura 4 y figura 5 representan las entidades definidas en el diseño de la base de datos, se tuvo en cuenta que para conservar la integridad referencial, cada tabla posee un Id numérico y único, que a su vez sirve de llave principal y que permite distinguir cada registro en las diferentes tablas. En los anexos A al N se encuentra un diccionario de datos de cada una de las tablas creadas en la base de datos con su descripción detallada de cada uno de sus campos.

Figura 4. Entidades

[58] IZQUIERDO, Luís, Introducción a la Programación Orientada a Objetos.[En línea], [consultado el 23 de octubre de 2016]. Disponible en: http://luis.izqui.org/ resources/ ProgOrientadaObjetos.pdf

Figura 5. Entidades definidas en la base de datos



Fuente: Autores

7.2 PROCEDIMIENTOS ALMACENADOS.

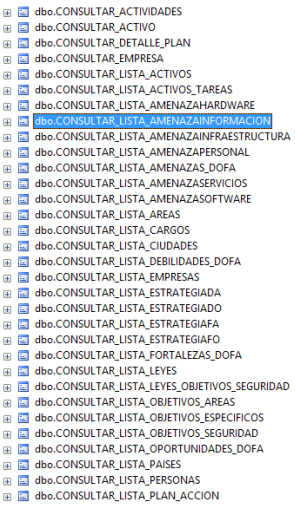
Conjunto de comandos que pueden ser ejecutados directamente en el servidor de Base de Datos y no por el programa cliente que lo accede, permitiendo la ejecución de una acción o conjunto de acciones específicas.[59]

Usar procedimientos almacenados en lugar de concatenación de cadenas para construir consultas dinámicas desde los datos de entrada del usuario para todas las sentencias SQL reduce la posibilidad de ataques de inyección SQL[60] .

En el diseño de la base de datos del software prototipo se programarón diferentes procedimientos almacenados para el ingreso de información, consulta, modificación y eliminación de la misma. a continuación se realiza una corta descripción de los procedimientos almacenados.

7.2.1 Procedimiento almacenado consultar. En la figura 6 se pueden observar los procedimientos almacenados creados para realizar las diferentes consultas de datos, que se realizan a sus respectivas tablas. Estos procedimientos almacenados devuelven los registros de cada una de las tablas.

Figura 6. Crud Consultar



Fuente: Autores

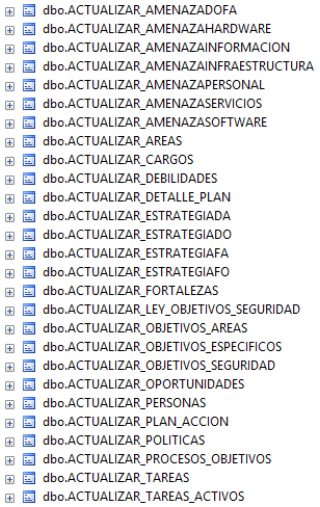
---

[59] ECURE. Procedimientos almacenados. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://www.ecured.cu/Procedimientos_almacenados

[60]SQL SHACK . Creando usando procedimientos almacenados. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: http://www.sqlshack.com/ es/ creando-usando-procedimientos-almacenados-crud/

7.2.2 Procedimiento almacenado actualizar En la figura 7 se pueden observar los procedimientos almacenados creados para realizar las diferentes consultas de actualización de datos. Serán utilizados para actualizar la información de los registros existentes en las diferentes tablas.

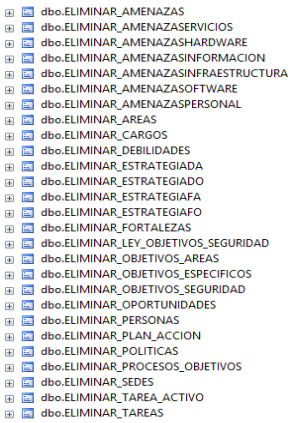
Figura 7. Crud Actualizar



Fuente: Autores

7.2.3 Procedimiento almacenado eliminar En la figura 8 se pueden observar los procedimientos almacenados creados para realizar las diferentes consultas de eliminación de datos. Con ellos se pretende eliminar un registro de una determinada tabla en la base de datos.

Figura 8. Crud Eliminar



Fuente: Autores

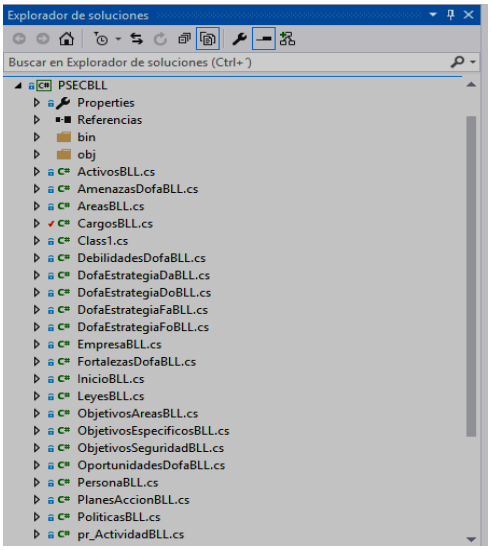
8. DISEÑO DEL PROTOTIPO Y ARQUITECTURA DEL SOFTWARE

En la fase de diseño del protipo se plasman los requerimientos de programación y se diseña una interfaz sencilla, pero practica a la hora de modelar la estructura funcional del software. para ello se programa el prototipo con el software visual studio .net lenguaje C# y base de datos Sqlserver 2014. En la programación orientada a objetos (POO), un objeto viene siendo la representación en un programa de un concepto y contiene toda la información necesaria para abstraerlo, son datos que describen sus atributos y operaciones que se pueden realizar sobre los mismos.[61] La arquitectura del software planteado para el diseño del prototipo se basa en el modelo por capas y entidades así:

- Capa de negocio: con lleva la lógica de negocio
- Capa de datos: se maneja la información de la base de datos
- Capa de presentación: capa con la cual interactúan los usuarios
- Entidades manejo por objetos.

8.1 Capa de negocio. En la figura 9 se puede observar las clases creadas para la capa de negocio. En ella se incluye toda la lógica de negocio de la aplicación.

Figura 9. Clases de la capa de Negocio

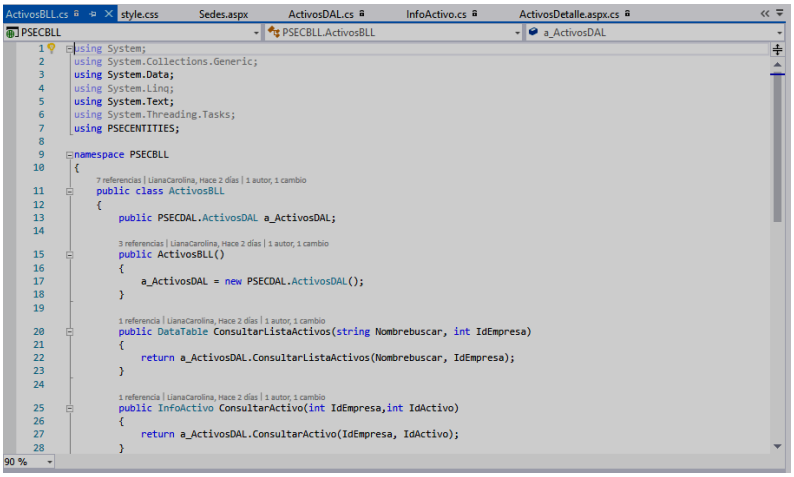


Fuente: Autores

[61] IZQUIERDO, Luís. Op. Cot. p. 20

8.1.1 Código de programación capa de negocio En la figura 10 se puede observar una parte del código de programación generado para la capa de negocio.

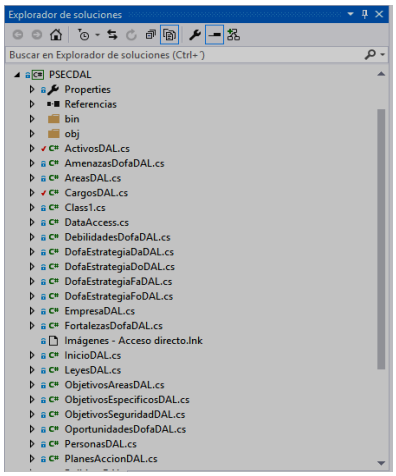
Figura 10. Código capa negocio



Fuente: Autores

8.2 Capa de datos. En la figura 11 se puede observar las clases creadas para la capa de datos. Tiene que ver con todo lo referente a la conexión con la base de datos y el llamado a los diferentes procedimientos almacenados.

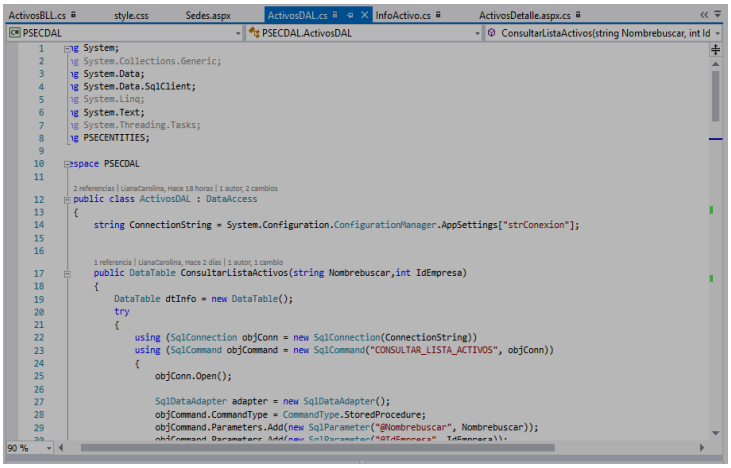
Figura 11. Clases de la capa de datos



Fuente: Autores

8.2.1 Código de programación capa de datos En la figura 12 se puede observar una parte del código de programación generado para la capa de datos.

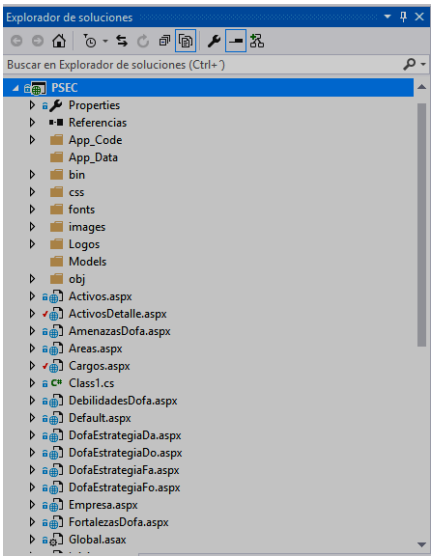
Figura 12. Código de la capa de datos



Fuente: Autores

8.3 Capa de presentación. En la figura 13 se puede observar las clases creadas para la capa de presentación. Hace referencia a la parte visual o lo que se le presenta al usuario final de la aplicación conocido también como Front-end.

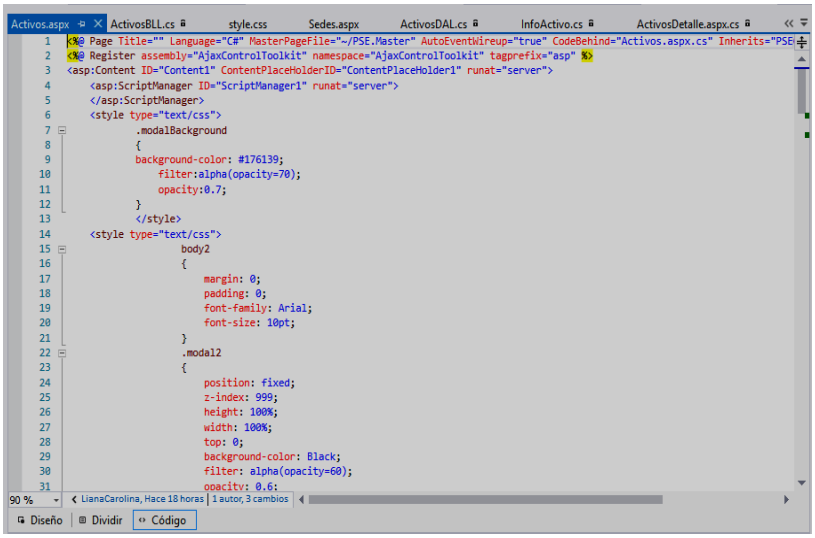
Figura 13. Capa de presentación



Fuente: Autores

8.3.1 Código de programación capa de presentación En la figura 14 se puede observar una parte del código de programación generado para la capa de presentación.

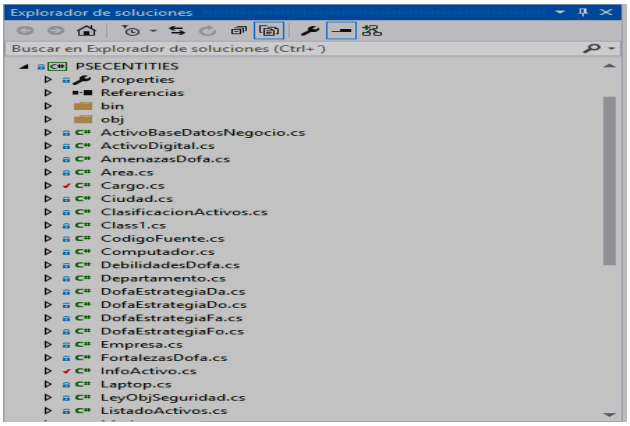
Figura 14. Código capa presentación



Fuente: Autores

8.4 Capa de entidades. En la figura 15 se puede observar las clases creadas para la capa de entidades.

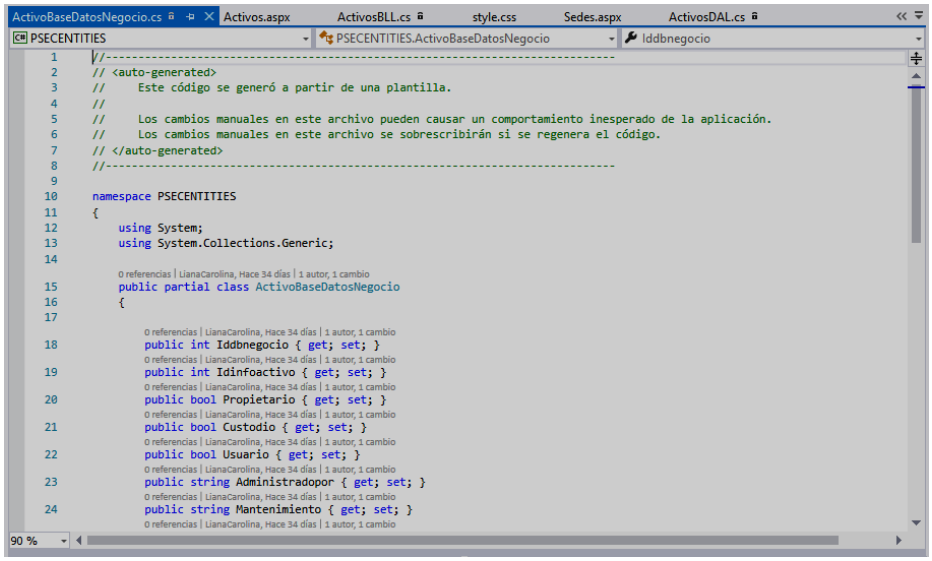
Figura 15. Entidades



Fuente: Autores

8.4.1 Código de programación capa de entidades En la figura 16 se puede observar una parte del código de programación generado para la capa de entidades.

Figura 16. Código entidades



Fuente: Autores

9. PRUEBAS DEL PROTOTIPO

Una vez se ha pasado por las diferentes etapas del software, se llega a obtener un producto representado en un software inicialmente la primera prueba se denomina prueba unitaria o de componente, este tipo de prueba es ejecutada normalmente por el equipo de desarrollo y consiste en la ejecución de la actividades que le permitan verificar al desarrollador que los componentes unitarios programados están codificados bajo condiciones de robustez, esto es soportando el ingreso de datos erróneos o inesperados y demostrando así la capacidad de tratar errores de manera controlada. [62]

Es un procedimiento usado para validar que un módulo o método de un objeto fuente funciona apropiadamente y en forma independiente. A través de ellas se verifica que cierto módulo o método se ejecuta dentro de los parámetros y especificaciones concretadas en documentos tales como los casos de uso y el diseño detallado, permiten detectar efectivamente la inyección de defectos durante fases sucesivas de desarrollo o mantenimiento.[63]

A continuación, se mostrarán algunas imágenes representativas de los módulos que integran el software prototipo y las pruebas realizadas con la información que suministra la empresa y que ha sido ingresada en los diferentes formularios.

9.1 PRUEBAS FUNCIONALES DEL PROTOTIPO DE SOFTWARE

En la realización de las pruebas al prototipo de software propuesto en la tesis se contó con el apoyo y confianza de la empresa Ingeltrosystemas ies Ltda. Constituida en la Cámara de Comercio el 17 de mayo de 1984. Compañía dedicada a la venta de partes y accesorios para equipos de cómputo, desktop, servidores, plotters, impresoras, portátiles, scanners, proyectores, tablet, pcs, cámaras digitales, fax, configuraciones, redes, accesorios, consumibles, papelería, así mismo a la prestación de servicios de mantenimiento preventivo y correctivo y desarrollo de software a la medida.
Para la realización de las pruebas del software y asesoría en seguridad de la información se realizaron varias reuniones con el gerente de la compañía y una presentación formal de los beneficios que la empresa podría llegar a adquirir al usar el software prototipo para establecer un gobierno de seguridad de la información, luego de esta reunión se acordó un plan de trabajo para realizar las

[62] WORDPRESS. Pruebas del software. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://pruebasdelsoftware.wordpress.com/
[63] KYBELE. Herramientas y material de pruebas para software [En línea], [consultado el 23 de octubre de 2016]. Disponible en: http://www.kybele.etsii.urjc.es/docencia/IS_LADE/2011 2012/Material/Pruebas%20de%20SoftwareHerraminetas.pdf

pruebas del software prototipo para ello se contó con la colaboración de las áreas gerenciales de la empresa y de sus trabajadores y el acompañamiento por parte nuestra para ingresar la información en los diferentes módulos de la aplicación.

La primera parte de la prueba se basó en reuniones con el área administrativa quien proporciono la información general de la empresa, a raíz de esta primera reunión se propone congregar a los líderes cabezas de áreas quienes asignaron a una persona para que colaborara con la labor que se había estipulado. En las reuniones de recolección de la información se realizó una presentación formal del esquema de trabajo a los colaboradores que la empresa había asignado se les explico la importancia de la labor que ellos iban a cumplir y se inició el proceso de recolección e ingreso de la información al prototipo de software en los diferentes formularios iniciando por la definición del dofa en seguridad de la información, la descripción de las diferentes áreas que conforman el organigrama empresarial, definición de los objetivos de las áreas de la empresa, descripción de los procesos que la empresa maneja, información de las personas a cargo de esos procesos, una identificación de los activos estratégicos basados en los principios de confidencialidad, integridad y disponibilidad de los mismos, establecer los objetivos de seguridad planes propuestos políticas de seguridad de la información, estrategias de seguridad de la información y por último la generación de los reportes.

A continuación, se presentarán las pruebas realizadas al prototipo por cada módulo propuesto en el diseño del software como son:

- Formulario empresa
- Formulario sedes
- Formulario debilidades, oportunidades, fortalezas, amenazas, estrategias
- Formulario áreas
- Formulario objetivos de negocio
- Formulario procesos
- Formulario cargos
- Formulario personas
- Formulario activos
- Formulario Políticas
- Formulario Planes
- Formulario estrategias

9.1.1 Formulario empresa. La información de este módulo fue facilitada e ingresada con nuestro acompañamiento por el área de la gerencia administrativa.

El formulario descrito se puede observar en la figura 17.

Figura 17. Formulario empresa

Fuente: Autores

9.1.2 Formulario sedes. La información de este módulo fue facilitada e ingresada con nuestro acompañamiento por el área de la gerencia administrativa.

En este formulario se debe ingresar la información de las sedes de la empresa como tipo de sede, país, ciudad, nombre de la sede, dirección, teléfono, número del móvil y un e-mail de contacto. este formulario descrito se puede observar en la figura 18, con este formulario se pretende tener conocimiento de la organización y su contexto empresarial.

Figura 18. Sedes

Fuente: Autores

9.1.3 Formulario debilidades. La información de este módulo fue facilitada e ingresada con nuestro acompañamiento por el área de la gerencia de tecnología y la gerencia administrativa.

En este formulario se debe ingresar la información correspondiente al Dofa en seguridad de la información en el formulario que se observa en la figura 19 se puede apreciar un listado de las posibles debilidades encontradas en materia de seguridad de la información en la empresa ies.

Figura 19. Debilidades

Fuente: Autores

9.1.4 Formulario oportunidades. La información de este módulo fue facilitada e ingresada con nuestro acompañamiento por el área de la gerencia de tecnología y gerencia administrativa.

En este formulario se debe ingresar datos de las oportunidades que tiene la empresa en cuestiones de seguridad de la información tal como se puede observar en la figura 20. El formulario se diseño para permitir actualizar las leyes Colombianas en temas de seguridad de la información y presentarlas como una opción de oportunidad que la empresa ies puede llegar a contemplar para fortalecer sus niveles de seguridad.

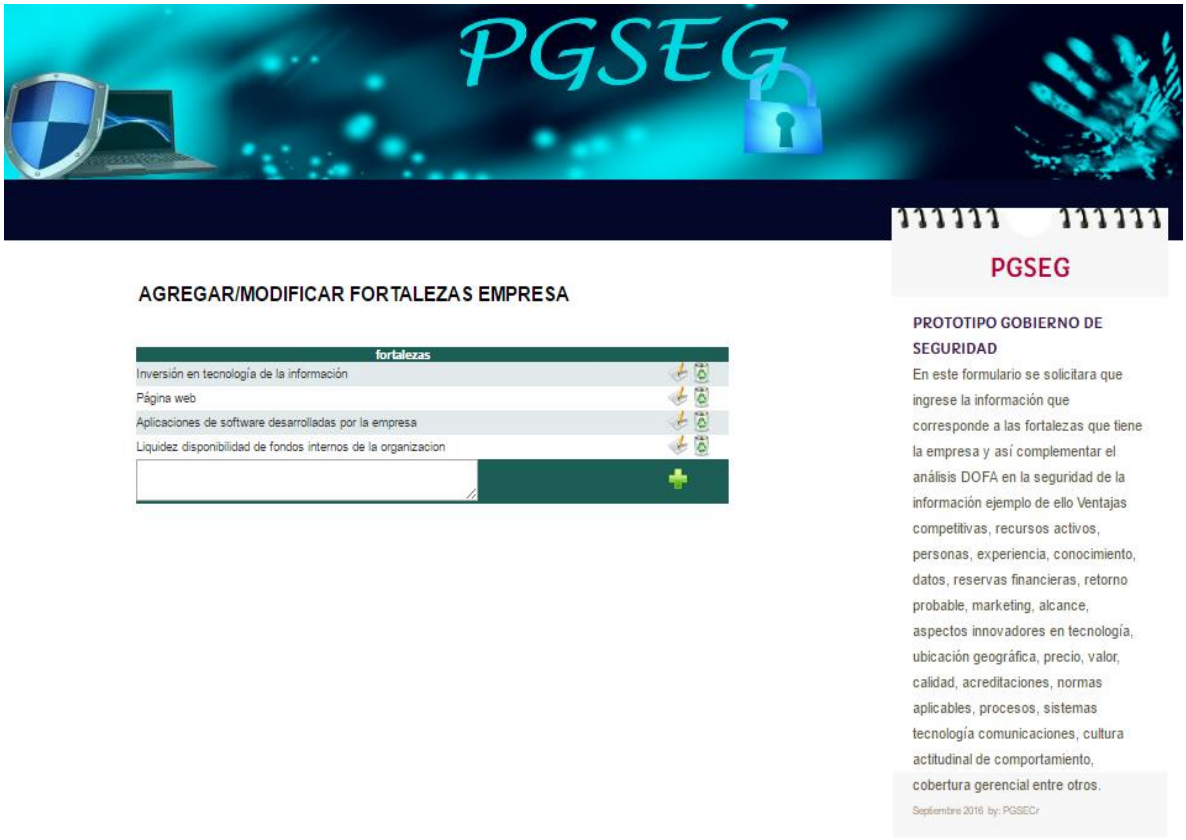
Figura 20. Oportunidades

Fuente: Autores

9.1.5 Formulario fortalezas. La información de este módulo fue facilitada e ingresada con nuestro acompañamiento por el área de la gerencia de tecnología y gerencia administrativa.

En este formulario se debe ingresar la información Fortalezas que la empresa ies tiene a niveles de infraestructura, tecnología y a niveles económicos que la distinguen de otras empresas y que pueden llegar a fortalecer los niveles de seguridad de la información de la empresa. En la figura 21 se pueden llegar a observar las fortalezas identificadas por ies ltda.

Figura 21. Fortalezas



Fuente: Autores

9.1.6 Formulario amenazas. La información de este módulo fue facilitada e ingresada con nuestro acompañamiento por el área de la gerencia de tecnología y gerencia administrativa.

En este formulario se recopilan las posibles amenazas en seguridad de la información que pueden llegar a materializarse en ies ltda si no se llegaran a tomar los controles adecuados, entre los cuales es importante mencionar fortalecer la empresa en las debilidades encontradas en la infraestructura, la tecnología, en los procesos, en el personal y en las politicas generadas en pro de la seguridad de la información. En la figura 22 se puede observar un listado detallado de las amenazas identificas por la empresa ies.

Figura 22. Amenazas

Fuente: Autores

9.1.7 Formulario áreas. La información de este módulo fue facilitada e ingresada con nuestro acompañamiento por el área de la gerencia administrativa.

En este formulario se debe ingresar la información de las áreas que conforman la estructura organizacional de ies, asi mismo deben quedar estipulados los nombres de los comités designados para el establecimiento del plan de seguridad de la información en ies. Como se puede llegar a observar en la descripción del formulario en la figura 23

Figura 23. Áreas

Fuente: Autores

9.1.8 Formulario objetivos negocio. La información de este módulo fue facilitada e ingresada con nuestro acompañamiento por el área de la gerencia administrativa.

Este formulario ha sido diseñado para el ingreso de los objetivos que el negocio propone en temas de seguridad de la información en la empresa ies ltda, estos objetivos se pueden observar en la figura 24.

Figura 24. Objetivos de Negocio

Fuente: Autores

9.1.9 Formulario procesos objetivos. La información de este módulo fue facilitada e ingresada con nuestro acompañamiento por cada área gerencial.

En este formulario se debe ingresar la información de los procesos que la empresa ies propone en temas relacionados con la seguridad de la información y su orden de importancia. Esto se puede observar en la figura 25.

Figura 25. Procesos por objetivos

Fuente: Autores

9.1.10 Formulario cargos procesos. La información de este módulo fue facilitada e ingresada con nuestro acompañamiento por cada área gerencial.

En este formulario se debe ingresar la información de los procesos de la empresa representado en el nivel de importancia la dependencia a la cual corresponde y el cargo asignado tal como se puede apreciar en la figura 26.

Figura 26. Procesos

Fuente: Autores

9.1.11 Formulario personas cargos. La información de este módulo fue facilitada e ingresada con nuestro acompañamiento por el área de la gerencia administrativa.

En este formulario se debe ingresar la información de las personas y los cargos asignados para el cumplimiento del programa de seguridad de la información en la empresa ies ltda. Tal como se puede observar en la figura 27.

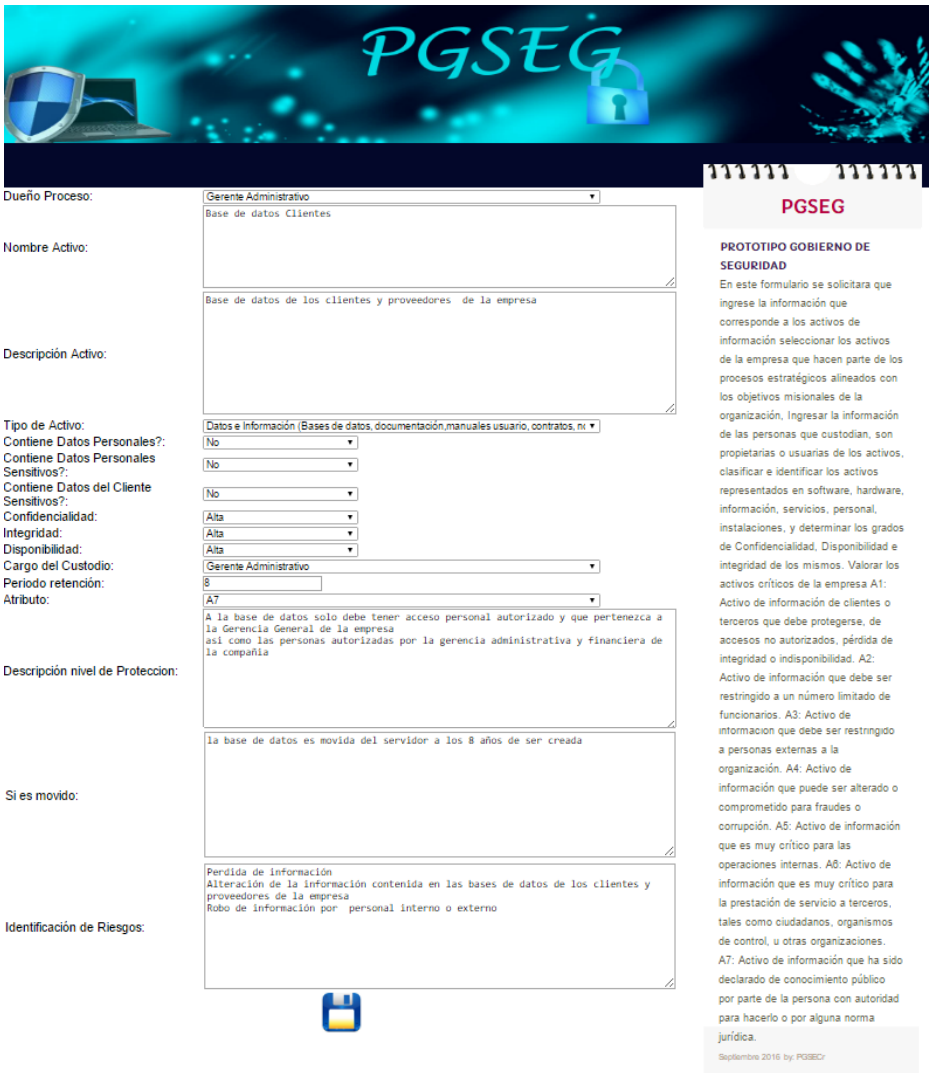
Figura 27. Personas por cargos

Fuente: Autores

9.1.12 Formulario activos. La información de este módulo fue facilitada e ingresada con nuestro acompañamiento por el área de la gerencia administrativa.

En este formulario se debe ingresar la información correspondiente a la identificación de los activos de información de la empresa en el formulario al lado izquierdo se puede encontrar una guia de como completar la información solicitada para la identificación de los activos críticos. Tal como se puede observar en la figura 28.

Figura 28. Identificación Activos



Fuente: Autores

9.1.13 Formulario lista activos. La información de este módulo fue facilitada e ingresada con nuestro acompañamiento por el área de la gerencia administrativa.

En este formulario se debe ingresar la información de la lista de los activos críticos de información, para ello se debe asignar una persona responsable la cual será la encargada de salvaguardar la información de los activos críticos de información en la empresa ies ltda. En la figura 29 se puede observar el formulario lista de activos.

Figura 29. Formulario lista activos

Fuente: Autores

9.1.14 Formulario objetivos de seguridad. La información de este módulo fue facilitada e ingresada con nuestro acompañamiento por el área de la gerencia administrativa.

En este formulario se debe ingresar la información de los objetivos de seguridad que la empresa debe adoptar tal como se puede observar en la figura 30.

Figura 30. Objetivos de Seguridad

Fuente: Autores

9.1.15 Formulario políticas de seguridad. La información de este módulo fue facilitada e ingresada con nuestro acompañamiento por el área de la gerencia administrativa, gerencia de tecnología.

En este formulario se debe ingresar la información de las políticas de seguridad propuestas para ser aprobadas por los altos directivos de la empresa tal como se puede observar en la figura 31.

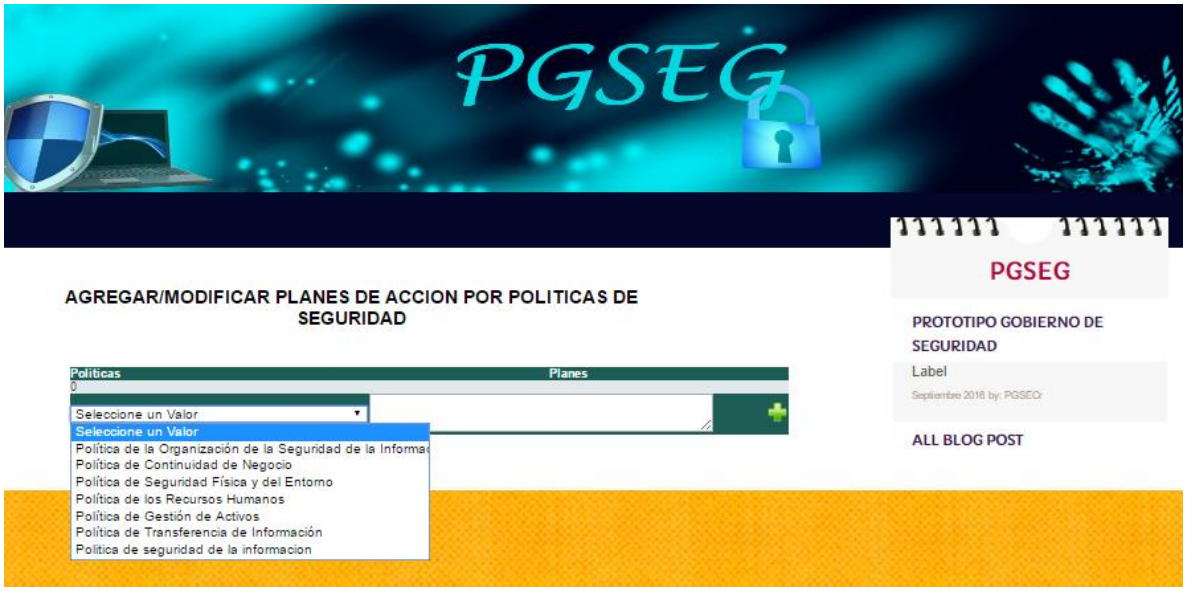
Figura 31. Políticas de Seguridad

Fuente: Autores

9.1.16 Formulario planes de acción. La información de este módulo fue facilitada e ingresada con nuestro acompañamiento por el área de la gerencia administrativa, gerencia de tecnología.

En este formulario se debe ingresar la información correspondiente a los planes de acción en seguridad que la empresa debe adoptar en beneficio de mejorar o instaurar un gobierno de seguridad de la información, Este formulario se puede observar en la figura 32.

Figura 32. Planes de Acción



Fuente: Autores

9.1.17 Formulario estrategias. La información de este módulo fue facilitada e ingresada a la aplicación con el apoyo de la gerencia administrativa y gerencia de tecnología.

En este formulario se debe ingresar la información correspondiente a las estrategias que la empresa debe asumir en beneficio de un adecuado gobierno de seguridad de la información tal como se puede observar en la figura 33.

Figura 33. Estrategias de Seguridad

Fuente: Autores

9.1.18 Resultados e impactos esperados. La idea de realizar esta tesis se basó prácticamente en la necesidad de plantear una nueva opción de facilitar la recopilación de información de las empresas para ser analizada posteriormente por el oficial de seguridad, con esta propuesta se quiere llegar a hacer parte de esta labor a la empresa en general, cada individuo cada proceso cada área cada persona íntegra el contexto empresarial desde la parte más fuerte del organigrama hasta la parte más sensible del mismo cada uno aporta su conocimiento en beneficio de la empresa para hacer que ella crezca en clientes, servicios opciones del mercado, en su buen nombre y reconocimiento hacia el exterior. es por ello que las personas son indispensables en esta labor ellos tienen conocimiento, tienen unas funciones definidas en la empresa, quien más que ellos pueden brindar información real y actualizada; la idea del software prototipo es ofrecer una herramienta de apoyo tanto a una consultoría como al oficial de seguridad de la información el cual se evitaría perder tiempo en la recopilación de la información.

Una guía importante es el resultado de una serie de investigaciones académicas que se ponen en práctica dentro una empresa u organización, tomando como base el gobierno corporativo el cual es constituido dentro de una empresa u organización, entendiendo que la seguridad de la información va transversal a toda la organización y su gestión debe ser respaldada por los altos directivos de la empresa en pro de un buen gobierno de seguridad de la información.

Al realizar las pruebas del software prototipo con información real de una empresa vemos que el acompañamiento del oficial de seguridad es indispensable en el levantamiento de información por su formación y experticia y que los altos directivos de las empresas deben ser un apoyo constante para el oficial de seguridad de la información ya que pondrán a su disposición las personas idóneas para la labor que se llegue a requerir. El software prototipo ofrece ayudas básicas para el ingreso de la información en el sistema, esto facilita un poco la identificación de qué tipo de información debe ingresarse y en que parte del sistema debe hacerse.

Por otro lado, los informes generados por la aplicación satisfacen las expectativas de funcionalidad del prototipo y arrojan la información esperada para el establecimiento de un gobierno de seguridad de la información.

El prototipo de software propuesto llega a ser una buena herramienta de trabajo para el oficial de seguridad, no obstante, en el alcance de la propuesta de tesis quedó estipulado que el enfoque de la tesis y del prototipo solo va hasta antes del análisis de riesgos, aunque en la propuesta se llega a valorar los activos de información como un insumo importante en el análisis de riesgo, la programación modular del prototipo y la estructura del software permitirá en futuras versiones realizar un análisis de riesgos completo al tener nuevos módulos enfocados en la continuidad del negocio.

10. REPORTES DEL GOBIERNO DE SEGURIDAD

El objetivo principal de esta sección, es la de encontrar un valor importante en la decisiones gerenciales del gobierno corporativo de una organización o empresa, por ende se desea entregar una información adecuada y estratégica, que a medida que se va parametrizando el software prototipo los resultados entregados por los reportes que son insumos estratégicos para el consultor o el oficial de seguridad de la información, y estos se verán reflejados en los informes para la alta dirección de la organización o empresa.

En la parametrización y la integración a nivel de consultas Transact-SQL se pueden obtener los reportes que permitirán un resumen de la información importante desde una perspectiva gerencial, el cual se incluye el análisis DOFA propuesto por el software prototipo, un inventario de activos de información, donde se incluye una valoración para determinar el nivel de criticidad que será un insumo importante para la gestión de riesgos que designe la organización o empresa y por ultimo un reporte sobre las políticas de seguridad generadas, las cuales estarán alineadas a los objetivos estratégicos de la organización o empresa[64].

10.1 ANÁLISIS DOFA

Los riesgos de la información están presentes cuando confluyen dos elementos: amenazas y vulnerabilidades. Las amenazas y vulnerabilidades están íntimamente ligadas, y no puede haber ninguna consecuencia sin la presencia conjunta de éstas. Las amenazas deben tomar ventaja de las vulnerabilidades y pueden venir de cualquier parte, interna o externa. Relacionada con el entorno de las organizaciones.[65]

El análisis Dofa a su vez nos permite identificar la situación actual en la que la empresa se encuentra, las estrategias actuales que la tienen en el mercado y la identificación de las políticas empresariales y aquellos aspectos que se relacionan con la seguridad de la información.

El análisis dofa involucra 4 conceptos fundamentales como son las debilidades, oportunidades, fortalezas y amenazas de las cuales se obtienen unas estrategias. A continuación se dará una breve descripción del análisis dofa en el prototipo.

---

64 ISACA. Op. Cit. p. 32

65 LA ORGANIZACIÓN INTERNACIONAL DE ESTANDARIZACIÓN. Tecnología De La Información – Técnicas De Seguridad – Código Para La Práctica De La Gestión De La Seguridad De La Información. USA: Estándar Internacional ISO/IEC 17799. Comité Técnico Conjunto ISO/IEC JTC 1

10.1.1 Fortalezas. Ventajas competitivas, recursos activos, personas, experiencia, conocimiento, datos, reservas financieras, retorno probable, marketing, alcance, aspectos innovadores en tecnología, ubicación geográfica, precio, valor, calidad, acreditaciones, normas aplicables, procesos, sistemas tecnología comunicaciones, cultura actitudinal de comportamiento, cobertura gerencial entre otros.[66]

10.1.2 Debilidades. Brechas en la capacidad, falta de fuerza competitiva, reputación, presencia y alcance, aspectos financieros, vulnerabilidades propias conocidas, confiabilidad de los datos, motivación, compromiso, liderazgo, no contar con acreditaciones, debilidades en procesos, tecnología y sistemas, debilidades gerenciales[67].

10.1.3 Oportunidades. Desarrollo del mercado, vulnerabilidades de la competencia, tendencias de la industria o estilo de vida, desarrollos tecnológicos e innovaciones, influencias globales, nuevos mercados, mercados objetivo, exportación, importación, nuevas propuestas de venta, leyes que se puedan adoptar, tácticas, desarrollo de productos negocios servicios, información e investigación, adopción de nuevas tecnologías, adopción de nuevos procesos.

10.1.4 Amenazas. Efectos políticos, efectos legislativos, desarrollo de ti, intensiones de los competidores, demanda del mercado, nuevas tecnologías, servicios, ideas, amenazas del ambiente exterior.[68]

10.1.5 Estrategias. Se combinan las fortalezas con las oportunidades para obtener estrategias fo, se combinan las fortalezas con las amenazas para obtener estrategias fa, se combinan las debilidades con las oportunidades para obtener estrategias do y por último se combinan las debilidades con las amenazas para obtener estrategias da.[69]

---

[66] FLÓREZ, Edward. Análisis FODA,.[En línea], [consultado el 23 de octubre de 2016]. Disponible en: http://es.slideshare.net/jcfdezmx2/que-es-el-analisis-foda-217430.

[67] Ibíd.

[68] LA ORGANIZACIÓN INTERNACIONAL DE ESTANDARIZACIÓN. Op. Cit. p. 69

[69] https://lcestrategia.wordpress.com/2015/01/26/matriz-dofa/

Una vez ingresada la información del Dofa se podrá obtener el primer informe, este permitirá identificar las Amenazas a las cuales están expuesta las empresas, las vulnerabilidades identificadas como los fallos internos en seguridad que la organización presenta, las debilidades que llegan a comprometer la seguridad de los activos de información de una empresa, las fortalezas representadas en las oportunidades que el mercado ofrece para la protección de los activos de información y la seguridad de los mismos. Este primer informe se puede observar en la figura 34.

Figura 34. DOFA de Seguridad

DOFA EN SEGURIDAD DE LA INFORMACIÓN

INTERNAS

Fortalezas
Inversión en tecnología de la información
Página web
Aplicaciones de software desarrolladas por la empresa
Liquidez disponibilidad de fondos internos de la organizacion

Debilidades
No hay Realización de planes de mejoramiento en el área TI
No hay programas de capacitación en seguridad de la información
No hay establecidos planes en seguridad de la información
No se realizan capacitaciones a los empleados en herramientas tecnológicas y seguridad informática
No hay programadas auditorias internas orientadas a la seguridad de la información

EXTERNAS

Oportunidades
Disposición de infraestructura tecnológica
Fuentes de financiación propias
Ética profesional y empresarial
Cumplimientos jurídicos y legales
Implantar un SGSI basados en la Norma ISO 27001:2013
Acogerse a la legislación que ofrece el decreto de ley Estatutaria 1581 del 2012 en lo que se refiere a protección de datos Personales

Estrategia Fo
Adaptarse a nuevos entornos
Mejoramiento de la comunicación entre organizaciones del mismo sector
Fortalecimiento de la cultura organizacional
Adoptar buenas practicas en el desarrollo seguro de aplicaciones y páginas web

Estrategia Do
Formar al personal en auditoria de sistemas, seguridad de la información y Riesgos asociados a la seguridad de la informacion
Definir lineamientos de Ti perdurables con el tiempo
Búsqueda de formas o mecanismos para fortalecer la cultura de la seguridad informática

Amenazas
Políticas y programas de desarrollo en el sector de las tecnologías de la informacion y seguridad informatica
Efectos culturales sobre la organización
Implementación de buenas prácticas o marcos de trabajo en materia de seguridad informática y riesgos
Políticas de seguridad del pais

EstrategiaFa
Adaptación a la situación económica del pais
Implementar marcos como la iso 27001
Iniciar alineación con otros estándares del Mercado

Estrategia Da
Mejoramiento de la cultura de seguridad informática al interior de TI
Mejoramiento de los procesos de auditoria enfocándola al área de tecnología
Acogerse a los marcos legales y normatividad del pais

Fuente: Autores

10.2 INVENTARIO DE ACTIVOS DE INFORMACIÓN

Este informe involucra las siguientes consultas a nivel de base de datos, áreas, Procesos, Activos, Confidencialidad, Integridad y disponibilidad, valoración del activo identificados en el análisis DOFA.

El informe de activos estratégicos involucra la información de los procesos actuales y el entendimiento de proyectos en curso y sus prioridades como se puede observar en la figura 35.

Figura 35. Inventario de activos

ACTIVOS DE INFORMACIÓN

Cargo Asignado	Nombre Persona	Apellido	Proceso	Orden importancia	Nombre Activo	Descripcion Activo	Id Cargo Custodio
Gerente General	Marvin	Diaz	Realizar capacitaciones con los Jefes de Departamento y todo el personal.	1			
Gerente Administrativo	Dolly	Ramirez	Adecuación de espacio físico; energía eléctrica; aire acondicionado; protección contra incendios entre otros orientados a la seguridad de los activos de información	1	Base de datos Clientes	Base de datos de los clientes y proveedores de la empresa	29

Datospersonales	Datos Sensitivos Personales	Datos Sensitivos Cliente	Confidencialidad	Integridad	Disponibilidad
False	False	False	H	H	H

Atributo	Perido Retencion	Riesgos
A7	8	Perdida de información Alteración de la información contenida en las bases de datos de los clientes y proveedores de la empresa Robo de información por personal interno o externo

Fuente: Autores

10.3 POLÍTICAS DE SEGURIDAD Y ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN

Este reporte involucra las siguientes consultas a nivel de base de datos.

Teniendo en cuenta los objetivos de seguridad alineados con el gobierno corporativo de la Organización o Empresa, se plantea las políticas de seguridad basados en la norma ISO 27001:2013, el cual se establece los objetivos según como lo indica la norma mencionada, tanto la aplicabilidad, directrices y estándar dentro de cada política está sujeto al core del negocio de cada organización alineado a la visión, misión y objetivos empresariales.

En la siguiente figura 36 se muestra un modelo de las políticas de seguridad dentro del software prototipo.

Figura 36. Políticas de Seguridad según ISO 27001:2013

POLITICAS EN SEGURIDAD DE LA INFORMACION

Descripcion de la Política	Objetivo	Aplicabilidad	Directrices	Estandar
Política de la Organización de la Seguridad de la Información	Establecer un marco de referencia de gestión para iniciar y controlar la implementaci4 y la operación de la seguridad de la información dentro de la organización	Es la asignación de todas la responsabilidades de la seguridad de la información	Definición de las responsabilidades para cada una de las políticas que se generen dentro de la organización	Segregación de funciones, contacto con las autoridades, contactos con los grupos de interés especial
Política de Continuidad de Negocio	La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización	La organización debe determinar los requisitos mínimos para tener la continuidad del negocio.	Establecer, documentar e implementar procedimientos y controles para asegurar el nivel de continuidad, disponibilidad de las instlaciones.	El modo de aplicación de la política de seguridad dentro de una organización
Política de Seguridad Física y del Entorno	Prevenir el acceso físico no autorizado, el daño y la interferencia a la información a las instalaciones de procesamiento de información de la organización	Definir y usar unos perímetros de seguridad y usarlos para proteger las áreas que contengan información crítica	Controles de acceso físicos, seguridad de las oficinas, trabajo de áreas seguras, áreas de despacho y carga, seguridad del cableado, retiro de activos	El modo de aplicación de la política de seguridad dentro de una organización
Política de los Recursos Humanos	Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.	Es la verificación de antecedentes para los candidatos a un empleo	Definición de las funciones para cargo, capacitaciones y acuerdos de confidencialidad	El modo de aplicación de la política de seguridad dentro de una organización

Fuente: Autores

10.4 ESTRATEGIAS

Este reporte involucra las siguientes consultas a nivel de base de datos. Objetivos de Negocio, Objetivos de Seguridad, política de seguridad, relación de los recursos que cuenta la organización, el análisis de brecha de seguridad, estructura organizacional, roles y responsabilidades.

Informacion que se debe tener en cuenta para la definicion de la estrategia de seguridad.[70]

- Objetivos Especificos
- Relacion componentes, estrategico, tactico y operativo
- Analisis de brecha de seguridad
- Elementos de la estrategia
- Recursos
- Roles y responsabilidades
- Restricciones
- Implementación de la estrategia

[70]TIPSEGURIDADTIC. Planeación estratégica Seguridad.,. [En línea], [consultado el 23 de octubre de 2016]. Disponible enhttp://52.1.175.72/portal/sites/all/themes/argo/assets/img/ Pagina/16-PlaneacionEstrategicaSeguridad.pdf

10.5 MEDICIONES DEL GOBIERNO DE SEGURIDAD

Durante la implementación del gobierno de seguridad, se debe realizar una medición del estado de la ejecución del gobierno de seguridad en la organización o empresa, por tal razón se plantea los siguientes formatos como se puede observar en la figura 37.

- Plan de capacitación y sensibilización
- Plan de auditorías Internas
- Plan de mejora continua
- Matriz Raci (encargado, responsable, consultado, informado)

Figura 37. Matriz Raci

MATRIZ RACI

Proceso	Tarea	R Encargado	A Responsable	C Consultado	I Informado
Realizar capacitaciones con los Jefes de Departamento y todo el personal.	evlaluaciones de las capacitaciones	CIO en seguridad de la Información	Gerente General	Gerente General	Gerente General
Realizar capacitaciones con los Jefes de Departamento y todo el personal.	realizar autoevaluaciones sobre los expositores	CIO en seguridad de la Información	Gerente General	Finanzas y Contabilidad	Finanzas y Contabilidad
Coordinar la realización de Capacitaciones en seguridad de la información a todo el personal de la empresa incluyendo contratistas y personal de apoyo	Jugar un rol ejecutivo para asegurar que los riesg	CIO en seguridad de la Información	CIO en seguridad de la Información	Gerente General	Comité de dirección en seguridad de la informacion
Proceso de Monitoreo de accesos lógicos a bases de datos y aplicaciones	El uso de la infraestructura tecnológica en toda l	Gerencia Tecnologica	Gerencia Tecnologica	Gerente General	Comité de dirección en seguridad de la informacion

Fuente: Autores

11. CONCLUSIONES

Es viable la realización del software prototipo propuesto en la tesis, cumple con las expectativas de funcionalidad y parametrización de gobierno de seguridad ya que ha sido formulado bajo los parámetros de las normas ISO 27001:2013 y el Manual de Preparación para el Examen CISM de ISACA en el dominio del gobierno de seguridad.

La propuesta de la tesis se sale de los estereotipos de realizar un análisis en seguridad de la información exclusiva para una sola empresa propuestas planteadas en otros proyectos de grado. Nuestra propuesta incluye la realización de un producto para recolectar y permitir estructurar un gobierno de seguridad de la información siendo esta la base para establecer un SGSI a nivel empresarial y el prototipo se propone no solo para el análisis de una empresa si no para cualquier empresa que quiera establecer un gobierno de seguridad de la información que sea transversal al gobierno corporativo de la organización o empresa.

La propuesta de software prototipo al ser modular en su estructura de diseño programación y a niveles funcionales puede llegar a extenderse en la programación futura hacia el análisis de riesgos en seguridad de la información y puede llegar a ser la base para el desarrollo de un módulo de continuidad del negocio.

El análisis de las variables propuestas en el Manual de Preparación al Examen de CISM por ISACA nos permitió estructurar mejor el software a si mismo nos enriqueció en conocimiento y experiencia replanteándonos la forma más adecuada de plasmar las ideas que se tenían para la programación del prototipo, tan es así que al inicio se planteó la posibilidad de asignar responsables en las empresas para ingresar solo la información adecuada al software, información que solo compete al establecimiento de las funciones de las personas en la empresa, luego de analizar bien las diversas situaciones que se podrían llegar a presentar al ingresar la información en el software prototipo se replanteo el esquema de utilización con el acompañamiento siempre del oficial de seguridad de la información por el conocimiento y experticia que da el valor agregado, esto con el fin de ser un apoyo y ayuda para plasmar los datos solicitados en términos de la seguridad de la información. Por esta misma razón la creación de las ayudas en el software para ingresar únicamente la información solicitada y obtener buenos resultados en los reportes finales.

Los conceptos del gobierno de seguridad de la información han sido enriquecedores para nuestra formación como especialistas en seguridad informática y hacen parte de la experiencia futura a nivel laboral con la que debemos enfrentarnos.

BIBLIOGRAFÍA

ALTAMIRANO, Carlos. Modelo de Gobierno de seguridad de la información [Citado en: 21/06/2010] [En línea], [consultado el 23 de octubre de 2016]. Disponible en: http://www.magazcitum.com.mx/?p=212#.VkudTdgvfIU

ARCHIVO GENERAL DE LA NACIÓN, Compilación normativa 2014. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: <http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/SINAE/Productos%20SINAE%202013/Compilacion_Normativa.pdf>

CÁMARA VENEZOLANA DE EMPRESAS DE TECNOLOGÍAS DE INFORMACIÓN Gobernabilidad y seguridad de la información beneficios. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: http://www.cavedatos.net/eventos/? i=65>

CERT. Gestión de incidentes de seguridad de la información. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://www.cert.uy/.../politica+de+gestion+de+ incidentes+ (.pdf+602+KB). pdf.

CGH. Eventos Adversos. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: www.cgh.org.co/imagenes/calidad1.pdf

CODEJOBS. Vulnerabilidad. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: ¿Qué es vulnerabilidad? https://www.codejobs.biz/.../seguridad-**informatica**-que-es-una-**vulnerabilidad**- una-am.

DEBITOORS. ¿Qué son activos? [En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://debitoor.es/glosario/definicion-de-activos.

DEFINICIONES ABC ¿Qué es confidencialidad? [En línea], [consultado el 23 de octubre de 2016]. Disponible en: definicionABC.de/confidencialidad/

_____. ¿Qué es efectividad? [En línea], [consultado el 23 de octubre de 2016]. Disponible en: www.definicionabc.com › General

_____. ¿Qué es eficiencia? [En línea], [consultado el 23 de octubre de 2016]. Disponible en: definicionABC.de/eficiencia/

DEFINICIÓN MX. ¿Qué es cumplimiento? [En línea], [consultado el 23 de octubre de 2016]. Disponible en: definicion.mx/disponibilidad/

DIALNET. ¿Qué es seguridad organizacional? [En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://dialnet.unirioja.es/ descarga/ articulo/2498321.pdf

DICCIONARIO CONTABLE. ¿Qué es disponibilidad? [En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://es.diccionariocontable. com/doc/35643664/Definición-de-disponibilidad.

DWIGHT CHESTNUT. Análisis FODA de Seguridad, [En línea], [consultado el 23 de octubre de 2016]. Disponible en: www.ehowenespanol.com/analisis-foda-seguridad-sobre_145898//

ECURE. Procedimientos almacenados. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://www.ecured.cu/Procedimientos_almacenados

EVOLUTION IT. ¿Qué son eventos de la seguridad? [En línea], [consultado el 23 de octubre de 2016]. Disponible en: www.evolution-it.com.co/...**seguridad**/siem-**seguridad-de-la-informacion**

FLÓREZ, Edward. Análisis FODA. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: http://es.slideshare.net/jcfdezmx2/que-es-el-analisis-foda-217430.

GESTIOPOLIS. Seguridad informática. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: www.gestiopolis.com/procedimientos-de-**seguridad-informatica**-en-sitios-web

GOOGLE. Seguridad física y del entorno. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://sites.google.com/a/istpargentina. edu.pe/.../seguridad-fisica-y-del-entorno

INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Sistema de Gestión de la Seguridad de la Información. ISO/IEC 27001:2013. Bogotá D.C. 2013. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: intranet. bogotaturismo.gov.co/sites/intranet...gov.co/.../NTC-**ISO**-**IEC**%2027001 pdf

ICESI. ¿Qué es gestión del riesgo? [En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://www.icesi.edu.co/revistas/index.php/ estudios_ gerenciales/article/view/ .../html

INFORMÁTICA BÁSICA. Lo que tienes que saber sección Magazine Impacto de las TI. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: http://informaticabasica28.blogspot.com. co/2013/03/impacto-de-las-ti.html>

INSTITUTO POLITÉCNICO NACIONAL. Herramientas para hacking ético Simulación de intrusión Test de penetración pág. 5. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: <https://viclab.files.wordpress.com/ 2010/11/docfinal_pub.pdf>

INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA. Suplantación de identidad. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://www.incibe.es/search/ ?allSearch Field=suplantar+identidad>

INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Sistema de Gestión de la Seguridad de la Información. ISO/IEC 27001:2013. Bogotá D.C. 2013

INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Sistema de Gestión de la Seguridad de la Información. ISO/IEC 27001:2013. Bogotá D.C. 2013

INFOSEGUR. ¿Qué es integridad? [En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://infosegur.wordpress.com/tag/**integridad**/

ISACA. Manual de Preparación al Examen CISM 2014.Impreso en Estados Unidos de América. ISBN 978-1-60420-410-0

ISTAS. ¿Qué es evaluación de riesgos? [En línea], [consultado el 23 de octubre de 2016]. Disponible en: www.istas.net/web/index.asp?idpagina=

IZQUIERDO, Luís, Introducción a la Programación Orientada a Objetos. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: http://luis.izqui.org/ resources/ ProgOrientadaObjetos.pdf

KYBELE. Herramientas y material de pruebas para software [En línea], [consultado el 23 de octubre de 2016]. Disponible en: http://www.kybele.etsii.urjc.es/docencia/IS_LADE/ 2011 2012/Material/Pruebas%20de%20SoftwareHerraminetas.pdf

MINISTERIO DEL INTERIOR. ¿Qué significa eventos de seguridad de la información? [En línea], [consultado el 23 de octubre de 2016]. Disponible enwww.mininterior.gov.co/sites/.../OIP-2014-PSI-Especificas-5%20 **Comunicaciones**.doc

_____. Significado de gestión de comunicaciones y operaciones. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: www.mininterior. gov.co/sites/ .../OIP-2014-PSI-Especificas-5%20**Comunicaciones**.doc

MINISTERIO DE TECNOLOGÍA, INDUSTRIA Y COMERCIO. Gestión de activos de información, [En línea], [consultado el 23 de octubre de 2016]. Disponible en: www.mintic.gov.co/**gestion**/615/articles-5482_G5_**Gestion**_Clasificacion.pdf

NTC 27001:2013, Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos

ORGANIZACIÓN INTERNACIONAL DE ESTANDARIZACIÓN. Tecnología de la información – técnicas de seguridad – código para la práctica de la gestión de la seguridad de la Información Estándar Internacional ISO/IEC 17799. Comité Técnico Conjunto ISO/IEC JTC 1

PREZI.CON. Significado de Adquisición, mantenimiento y desarrollo de sistemas de información. 2012. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://prezi.com/.../tema-7-adquisicion-desarrollo-y-mantenimiento-de-los-sistemas-d

PROTEJETE. ¿Qué es Seguridad de la información?, [En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://protejete.wordpress.com/gdr_principal/**seguridad_ información_ protección**/

SCRIBD. Definición de confiabilidad. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://es.scribd.com/doc/35643664/**Definicion**-de-**Confiabilidad**

SEG.INFORMÁTICOS. Qué son riesgos informáticos. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: seg**informatica**1audisistem.jimdo.com/**riesgos**-**informáticos**/

SEGURIDAD ANGGIE. Blog Seguridad informática. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: http://seguridadanggie.blogspot.com.co/2011/11/confidencialidad.html

SEGURIDAD INFORMÁTICA. ¿Qué es amenaza informática? [En línea], [consultado el 23 de octubre de 2016]. Disponible en: www.seguridad**informatica**.unlu.edu.ar

SGSI. Blog especializado en sistemas de gestión de seguridad de la información Iso 2014 Gobernanza seguridad de la información 4 abril de 2014.: [En línea], [consultado el 23 de octubre de 2016]. Disponible en: http://www.pmg-ssi.com/2014/04/iso-27014-gobernanza-de-seguridad-de-la-informacion/>

SQL SHACK . Creando usando procedimientos almacenados. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: http://www.sqlshack.com/ es/ creando-usando-procedimientos-almacenados-crud/

TECNOSEGURO ¿Qué es un control de acceso? [En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://www.tecnoseguro.com/.../**control-de-acceso/** ¿-que-es-un-**control-de-acceso**.htm.

TIP SEGURIDAD TIC. Planeación estratégica Seguridad.,. [En línea], [consultado el 23 de octubre de 2016]. Disponible enhttp://52.1.175.72/portal/sites/all/themes/argo/ assets/img/ Pagina/16-PlaneacionEstrategicaSeguridad.pdf

UNIVERSIDAD DISTRITAL. ¿Qué son políticas de seguridad? En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://portalws.udistrital.edu.co/.../**politica_seguridad**/ .../**Politica**_para_**Seguridad_I**

WORDPRESS. Pruebas del software. [En línea], [consultado el 23 de octubre de 2016]. Disponible en: https://pruebasdelsoftware.wordpress.com/

ANEXOS

Anexo A Información general de la Empresa

Este anexo corresponde al diccionario de datos de Sqlserver; en el cuadro 9 se puede observar la información de la empresa.

Cuadro 9. Información general de la empresa

PK	Name	Type	Not Null	Unique	Len	Notes
True	Idempresa	int	True	True		Campo que identifica la empresa Es llave primaria de la tabla empresa
False	Idactividad	int	True	False		Campo que identifica la actividad económica de la empresa Es llave foránea de la tabla actividad
False	Nombre	varchar	True	False	50	Campo que almacena el nombre de la empresa
False	Nit	varchar	True	False	11	Campo que almacena el nit de la empresa
False	AnioCreacion	date	True	False		Campo que almacena el año de creación de la empresa
False	Numemple	int	True	False		Campo que almacena el número de empleados que trabajan en la empresa
False	Logo	image	True	False		Campo que almacena la imagen corporativa logo de la empresa
False	Misión	text	True	False		Campo que almacena la información misional de la empresa
False	Visión	text	True	False		Campo que almacena la información que corresponde a la visión que tiene la empresa
False	ObjGeneral	text	True	False		Campo que almacena el objetivo general que tiene la empresa
False	PolSeguridadInfo	text	True	False		Campo que almacena la información correspondiente a las políticas de seguridad establecidas en la empresa

Columns	Association
(Idempresa = Idempresa)	0..* Tbl_Area.FK_Tbl_Area_Tbl_Empresa 1 Tbl_Empresa.PK_Tbl_Empresa
(Idempresa = Idempresa)	0..* Tbl_Madurez.FK_Tbl_Madurez_Tbl_Empresa 1 Tbl_Empresa.PK_Tbl_Empresa
(Idempresa = Idempresa)	0..* Tbl_Sedes.FK_Tbl_Sedes_Tbl_Empresa 1 Tbl_Empresa.PK_Tbl_Empresa

Fuente: Autores

Anexo B. Tabla Sedes

Este anexo corresponde al diccionario de datos de Sqlserver; en el cuadro 10 se puede observar la información correspondiente a las sedes de la empresa.

Cuadro 10. Información Sedes de la empresa

PK	Name	Type	Not Null	Unique	Notes
True	Idsede	int	True	True	Campo que identifica la Sede Es llave primaria de la tabla sedes
False	Idempresa	int	True	False	Campo que identifica las sedes de la empresa Es llave foránea de la tabla empresa
False	Idtiposede	int	True	False	Campo que identifica el tipo de sedes Es llave foránea de la tabla tipo sedes
False	Idpais	int	True	False	Campo que identifica el país Es llave foránea de la tabla país
False	Iddepto	int	True	False	Campo que identifica el departamento en el que se encuentra la sede de la empresa Es llave foránea de la tabla departamento
False	Idciudad	int	True	False	Campo que identifica la ciudad en la que se encuentra la sede de la empresa Es llave foránea de la tabla ciudad
False	Idpersonas	int	True	False	Campo que identifica a las personas que trabajan en las sedes de la empresa Es llave foránea de la tabla personas
False	Nombre	varchar	True	False	Campo que almacena el nombre de la sede de la empresa
False	Direccion	varchar	True	False	Campo que almacena la dirección de la sede de la empresa
False	Teléfono	int	False	False	Campo que almacena el número de teléfono de la sede de la empresa
False	Celular	int	False	False	Campo que almacena el número del celular para comunicarse con las sedes de la empresa
False	Email	varchar	True	False	Campo que almacena el mail de contacto en la sede de la empresa
Columns			Association		
(Idempresa = Idempresa)			0..* 1		Tbl_Sedes.FK_Tbl_Sedes_Tbl_Empresa Tbl_Empresa.PK_Tbl_Empresa
(Idtiposede = Idtiposede)			0..* 1		Tbl_Sedes.FK_Tbl_Sedes_Tbl_pr_TipoSede Tbl_pr_TipoSede.PK_Tbl_pr_TipoSede

Fuente: Autores

Anexo C. Tabla Tipo Sede

Este anexo corresponde al diccionario de datos de Sqlserver; en el cuadro 11 se puede observar la información correspondiente al tipo de la sede y su descripción.

Cuadro 11. Información tipo sedes de la empresa

PK	Name	Type	Not Null	Unique	Notes
True	Idtiposede	int	True	True	Campo que identifica el tipo de la sede Es llave primaria de la tabla Tipo Sede
False	Descripción	varchar	True	False	Campo que almacena la descripción general del tipo de sede
Columns			Association		
(Idtiposede = Idtiposede)			0.. * Tbl_Sedes.FK_Tbl_Sedes_Tbl_pr_TipoSede 1 Tbl_pr_TipoSede.PK_Tbl_pr_TipoSede		

Fuente: Autores

Anexo D. Tbl_Personas

Este anexo corresponde al diccionario de datos de Sqlserver; en el cuadro 12 se puede observar la información correspondiente a la información de las personas que trabajan en la empresa.

Cuadro 12. Información personas

PK	Name	Type	Not Null	Unique	Len	Notes
True	Idpersonas	int	True	True	0	Campo que identifica a las personas que trabajan en la empresa
False	Idcargo	int	False	False	0	Campo que identifica el cargo de las personas que trabajan en la empresa
False	Nombre	varchar	True	False	50	Campo que almacena el nombre de las personas que trabajan en la empresa
False	Apellido	varchar	True	False	30	Campo que almacena el apellido de las personas que trabajan en la empresa
False	Usuario	varchar	True	False	30	Campo que almacena la información del usuario que trabajan en la empresa
False	Ubicación	varchar	True	False	30	Campo que almacena la ubicación de las personas que trabajan en la empresa
False	Codigoemple	varchar	False	False	20	Campo que almacena el código del empleado que trabaja en la empresa
False	Fecha ingreso	datetime	True	False	0	Campo que almacena la fecha de ingreso de la persona que trabaja en la empresa
False	Sexo	varchar	True	False	1	Campo que almacena el tipo de sexo al cual corresponde la persona que trabaja en la empresa
False	Fechainicontrato	datetime	False	False	0	Campo que almacena la fecha de iniciación del contrato de la persona que trabaja en la empresa
False	Horaingreso	datetime	False	False	0	Campo que almacena la hora de ingreso a laborar de las personas que trabajan en la empresa
False	Horasalida	datetime	False	False	0	Campo que almacena la hora de salida de las personas que trabajan en la empresa
False	Diaslaborales	varchar	False	False	50	Campo que almacena los días hábiles de trabajo de las personas en la empresa
False	Tipocontrato	varchar	False	False	50	Campo que almacena el tipo de contrato que tienen las personas que trabajan en la empresa
False	Activo	bit	False	False	0	
Columns			Association			
(Idcargo = Idcargo)			0..* Tbl_Personas.FK_Tbl_Personas_Tbl_Cargo 1 Tbl_Cargo.PK_Tbl_Cargo			
(Idpersonas = Idpersonas)			0..* Tbl_InfoActivo.FK_Tbl_InfoActivo_Tbl_Personas 1 Tbl_Personas.PK_Tbl_Personas			

Fuente: Autores

Anexo E. Tabla Tbl_Cargo

Este anexo corresponde al diccionario de datos de Sqlserver; en el cuadro 13 se puede observar la información correspondiente a los cargos de las personas que se encargaran de manejar los procesos de las diferentes áreas en la empresa.

Cuadro 13. Información cargo personas

PK	Name	Type	Not Null	Unique	Len	Notes
True	Idcargo	int	True	True	0	Campo que identifica el cargo de las personas que se van a encargar de manejar los procesos en las diferentes áreas de la empresa
False	Idproceso	int	False	False	0	Campo que identifica los procesos que se van a realizar en las áreas de la empresa
False	Nivel	int	True	False	0	Campo que identifica el rango por nivel de las personas en la empresa
False	Dependencia	int	True	False	0	Campo que identifica la dependencia de las personas en el cargo actual en la empresa
False	Descripcion	varchar	True	False	50	Campo que identifica la descripción general de los cargos de la empresa
Columns			Association			
(Idcargo = Idcargo)			0..* 1	Tbl_Personas.FK_Tbl_Personas_Tbl_Cargo Tbl_Cargo.PK_Tbl_Cargo		
(Idproceso = Idproceso)			0..* 1	Tbl_Cargo.FK_Tbl_Cargo_Tbl_Proceso Tbl_Proceso.PK_Tbl_Proceso		

Fuente: Autores

Anexo F. Tabla Tbl_Area

Este anexo corresponde al diccionario de datos de Sqlserver; en el cuadro 14 se puede observar la información correspondiente a la información correspondiente a los cargos de las personas que se encargaran de manejar los procesos de las áreas en la empresa.

Cuadro 14. Información áreas de la empresa

PK	Name	Type	Not Null	Unique	Len	Notes
True	Idarea	int	True	True		Campo que identifica el área de la empresa Es llave primaria de la tabla área
False	Idempresa	int	True	False	0	Campo que identifica a la empresa Es llave foránea de la tabla empresa
False	Descripcion	varchar	True	False	50	Campo que almacena una descripción general del área en la empresa

Name	Type	Columns	Notes
UQ_Tbl_Area_Idarea	Public	Idarea	
PK_Tbl_Area	Public	Idarea	
FK_Tbl_Area_Tbl_Empresa	Public	Idempresa	

Columns	Association
(Idarea = Idarea)	0..* Tbl_ObjArea.FK_Tbl_ObjArea_Tbl_Area 1 Tbl_Area.PK_Tbl_Area
(Idempresa = Idempresa)	0..* Tbl_Area.FK_Tbl_Area_Tbl_Empresa 1 Tbl_Empresa.PK_Tbl_Empresa

Fuente: Autores

Anexo G. Tabla Tbl_ObjArea

Este anexo corresponde al diccionario de datos de Sqlserver; en el cuadro 15 se puede observar la información de los objetivos de las áreas de la empresa.

Cuadro 15. Información objetivos área de la empresa

PK	Name	Type	Not Null	Unique	Notes
True	Idobjarea	int	True	True	Campo que identifica los objetivos de las áreas en la empresa
False	Idarea	int	True	False	Campo que identifica las áreas de la empresa
False	Descripción	varchar	True	False	Campo que almacena la descripción general de las áreas de la empresa
Name		Type	Columns		Notes
UQ_Tbl_ObjArea_Idobjarea		Public	Idobjarea		
PK_Tbl_ObjArea		Public	Idobjarea		
FK_Tbl_ObjArea_Tbl_Area		Public	Idarea		
Columns		Association			
(Idarea = Idarea)		0..* 1	Tbl_ObjArea.FK_Tbl_ObjArea_Tbl_Area Tbl_Area.PK_Tbl_Area		
(Idobjarea = Idobjarea)		0..* **1**	Tbl_ObjEspecifico.FK_Tbl_ObjEspecifico_Tbl_ObjArea **Tbl_ObjArea.PK_Tbl_ObjArea**		

Fuente: Autores

Anexo H. Tabla Tbl_Ob_Seguridad

Este anexo corresponde al diccionario de datos de Sqlserver; en el cuadro 16 se puede observar la información de los objetivos en seguridad definidos para la empresa

Cuadro 16. Información objetivos de seguridad de la empresa

PK	Name	Type	Not Null	Unique	Notes
True	Idobjespecifico	int	True	True	Campo que identifica el objetivo específico de las áreas de la empresa
False	Idobjarea	int	True	False	Campo que identifica los objetivos del área en la empresa
False	Descripción	nchar	True	False	Campo que almacena una descripción general de los objetivos de la empresa
Name		Type	Columns		
PK_Tbl_ObjEspecifico		Public	Idobjespecifico		
FK_Tbl_ObjEspecifico_Tbl_ObjArea		Public	Idobjarea		
Columns		Association			
(Idobjarea = Idobjarea)		0..* 1	Tbl_ObjEspecifico.FK_Tbl_ObjEspecifico_Tbl_ObjArea Tbl_ObjArea.PK_Tbl_ObjArea		
(Idobjespecifico		0..* 1	Tbl_Politicas.FK_Tbl_Politicas_Tbl_ObjEspecifico Tbl_ObjEspecifico.PK_Tbl_ObjEspecifico		
(Idobjespecifico		0..* **Tbl_ObjEspecifico.PK_Tbl_ObjEspecifico**	Tbl_Proceso.FK_Tbl_Proceso_Tbl_ObjEspecifico		

Fuente: Autores

Anexo I. Tabla Tbl_Proceso

Este anexo corresponde al diccionario de datos de Sqlserver; en el cuadro 17 se puede observar la información de los procesos de la empresa.

Cuadro 17. Información procesos de la empresa

PK	Name	Type	Not Null	Unique	Len	Notes
True	Idproceso	int	True	True	0	Campo que identifica los procesos de las áreas en la empresa
False	Idobjespecifico	int	True	False	0	Campo que identifica los objetivos específicos de las áreas de la empresa
False	Descripción	varchar	True	False	50	Campo que almacena una descripción general de los procesos de las áreas en la empresa
False	Ordenimportancia	int	True	False	0	Campo que almacena el orden de importancia de los procesos en las áreas de la empresa
Name		Type	Columns			
PK_Tbl_Proceso		Public	Idproceso			
FK_Tbl_Proceso_Tbl_Obj Especifico		Public	Idobjespecifico			
Columns		Association				
Idobjespecifico = Idobjespecifico)		0..* 1	Tbl_Proceso.FK_Tbl_Proceso_Tbl_ObjEspecifico Tbl_ObjEspecifico.PK_Tbl_ObjEspecifico			
(Idproceso = Idproceso)		0..* **1**	Tbl_Cargo.FK_Tbl_Cargo_Tbl_Proceso **Tbl_Proceso.PK_Tbl_Proceso**			

Fuente: Autores

Anexo J. Tabla Tbl_InfoActivo

Este anexo corresponde al diccionario de datos de Sqlserver; en el cuadro 18 se puede observar la información correspondiente a los activos de la empresa.

Cuadro 18. Información activos de información

PK	Name	Type	Not Null	Unique	Len	Notes
True	Idinfoactivo	int	True	True	0	Campo que identifica la información de los activos
False	Idlistado	int	True	False	0	Campo que identifica el listado de activos
False	Idintegridad	int	True	False	0	Campo que identifica la integridad de los activos
False	Iddisponibilidad	int	True	False	0	Campo que identifica la disponibilidad de los activos
False	Idpersonas	int	True	False	0	Campo que identifica las personas con los activos
False	IdClasificaactivo	int	False	False	0	Campo que identifica la clasificación de los activos
False	Datopersonal	bit	True	False	0	Campo que sirve para seleccionar el tipo de información que maneja el activo
False	Datosencitivopersonal	bit	True	False	0	Campo que sirve para seleccionar el tipo de información que maneja el activo
False	Datosencitivocliente	bit	True	False	0	Campo que sirve para seleccionar el tipo de información que maneja el activo
False	Custodio	bit	True	False		Campo que sirve para seleccionar el papel cumplen las personas encargadas de resguardar la información
False	Propietario	bit	True	False		Campo que sirve para seleccionar el papel cumplen las personas encargadas de resguardar la información
False	Usuario	bit	True	False		Campo que sirve para seleccionar el papel cumplen las personas encargadas de resguardar la información
False	Periodoretenciondato	decimal	True	False		Campo que almacena el tiempo de retención del activo en la empresa
False	Actualnivelproteccidondato	varchar	True	False	30	Campo que almacena el actual nivel de protección de los datos
False	Proteccioninfo	varchar	True	False	50	Campo que almacena el actual nivel de protección de los datos
False	Descripción	varchar	True	False	50	Campo que almacena la descripción de la información de los activos

Fuente: Autores

Cuadro 18. (Continuación)

Constraints

Name	Type	Columns	Notes
PK_Tbl_InfoActivo	Public	Idinfoactivo	
FK_Tbl_InfoActivo_Tbl_ClasificacionActivos	Public	IdClasificaactivo	
FK_Tbl_InfoActivo_Tbl_ListadoActivos	Public	Idlistado	
FK_Tbl_InfoActivo_Tbl_Personas	Public	Idpersonas	
Columns	Association		
(IdClasificaactivo = IdClasificaactivo)	0..* 1	Tbl_InfoActivo.FK_Tbl_InfoActivo_Tbl_ClasificacionActivos Tbl_ClasificacionActivos.PK_Tbl_ClasificacionActivos	
(Idinfoactivo = Idinfoactivo)	0..* 1	Tbl_ActivoBaseDatosNegocio.FK_Tbl_ActivoBaseDatosNegocio_Tbl_InfoActivo Tbl_InfoActivo.PK_Tbl_InfoActivo	
(Idinfoactivo = Idinfoactivo)	0..* 1	Tbl_ActivoDigital.FK_Tbl_ActivoDigital_Tbl_InfoActivo Tbl_InfoActivo.PK_Tbl_InfoActivo	
(Idinfoactivo = Idinfoactivo)	0..* 1	Tbl_CodigoFuente.FK_Tbl_CodigoFuente_Tbl_InfoActivo Tbl_InfoActivo.PK_Tbl_InfoActivo	
(Idinfoactivo = Idinfoactivo)	0..* 1	Tbl_Computador.FK_Tbl_Computador_Tbl_InfoActivo Tbl_InfoActivo.PK_Tbl_InfoActivo	
(Idinfoactivo = Idinfoactivo)	0..* 1	Tbl_Laptop.FK_Tbl_Laptop_Tbl_InfoActivo Tbl_InfoActivo.PK_Tbl_InfoActivo	
(Idinfoactivo = Idinfoactivo)	0..* 1	Tbl_Medios.FK_Tbl_Medios_Tbl_InfoActivo Tbl_InfoActivo.PK_Tbl_InfoActivo	
(Idinfoactivo = Idinfoactivo)	0..* 1	Tbl_Red.FK_Tbl_Red_Tbl_InfoActivo Tbl_InfoActivo.PK_Tbl_InfoActivo	
(IdinfoActivo = Idinfoactivo)	0..* 1	Tbl_Riesgo.FK_Tbl_Riesgo_Tbl_InfoActivo Tbl_InfoActivo.PK_Tbl_InfoActivo	
(Idinfoactivo = Idinfoactivo)	0..* 1	Tbl_Servidor.FK_Tbl_Servidor_Tbl_InfoActivo Tbl_InfoActivo.PK_Tbl_InfoActivo	
(Idinfoactivo = Idinfoactivo)	0..* 1	Tbl_Software.FK_Tbl_Software_Tbl_InfoActivo Tbl_InfoActivo.PK_Tbl_InfoActivo	
(Idinfoactivo = Idinfoactivo)	0..* 1	Tbl_UtilidadesSoporte.FK_Tbl_UtilidadesSoporte_Tbl_InfoActivo Tbl_InfoActivo.PK_Tbl_InfoActivo	
(Idlistado = Idlistado)	0..* 1	Tbl_InfoActivo.FK_Tbl_InfoActivo_Tbl_ListadoActivos Tbl_ListadoActivos.PK_Tbl_ListadoActivos	
(Idpersonas = Idpersonas)	0..* 1	Tbl_InfoActivo.FK_Tbl_InfoActivo_Tbl_Personas Tbl_Personas.PK_Tbl_Personas	

Fuente: Autores

Anexo K. Tabla Tbl_Tbl_TipoActivo

Este anexo corresponde al diccionario de datos de Sqlserver, en el cuadro 19 se puede observar la información correspondiente a los tipos de activos de información de la empresa.

Cuadro 19. Información tipo de activos de información

PK	Name	Type	Not Null	Unique	Notes
True	Idtipoactivo	int	True	True	Campo que identifica al tipo de activo
False	Idempresa	int	True	False	Campo que identifica la empresa
False	Descripción	varchar	True	False	Campo que almacena la descripción del tipo de activos
Name		Type	Columns	Notes	
UQ_Tbl_TipoActivo_Idtipoactivo		Public	Idtipoactivo		
PK_Tbl_TipoActivo		Public	Idtipoactivo		
Columns		Association			
(Idtipoactivo = Idtipoactivo)		0..* 1	Tbl_ListadoActivos.FK_Tbl_ListadoActivos_Tbl_TipoActivo Tbl_TipoActivo.PK_Tbl_TipoActivo		

Fuente: Autores

Anexo L. Tabla Tbl_ListadoActivos

Este anexo corresponde al diccionario de datos de Sqlserver, en el cuadro 20 se puede observar la información correspondiente a la lista de activos de información de la empresa.

Cuadro 20. Información lista de activos de información

PK	Name	Type	Not Null	Unique	Len	Notes
True	Idlistado	int	True	True		Campo que identifica el listado de activos de la empresa
False	Idtipoactivo	int	True	False		Campo que identifica el tipo de activo en la empresa
False	Tipoinfo	varchar	True	False	50	Campo almacena la información del tipo de activo
False	Descripcion	varchar	True	False	50	Campo que almacena la descripción del tipo de activo
Name		Type	Columns	Notes		
UQ_Tbl_ListadoActivos_Idlistado		Public	Idlistado			
PK_Tbl_ListadoActivos		Public	Idlistado			
FK_Tbl_ListadoActivos_Tbl_TipoActivo		Public	Idtipoactivo			
Columns		Association				
(Idlistado = Idlistado)		0..* 1	Tbl_InfoActivo.FK_Tbl_InfoActivo_Tbl_ListadoActivos Tbl_ListadoActivos.PK_Tbl_ListadoActivos			
(Idtipoactivo = Idtipoactivo)		0..* **1**	Tbl_ListadoActivos.FK_Tbl_ListadoActivos_Tbl_TipoActivo **Tbl_TipoActivo.PK_Tbl_TipoActivo**			

Fuente: Autores

Anexo M. Tabla Tbl_Madurez

Este anexo corresponde al diccionario de datos de Sqlserver, en el cuadro 21 se puede observar la información correspondiente al nivel de madures de la empresa en seguridad de la información.

Cuadro 21. Información nivel de madurez de la empresa en seguridad

PK	Name	Type	Not Null	Unique	Notes
True	Idmadurez	int	True	True	Campo que identifica la tabla madurez
False	Idnivel	int	True	False	Campo que identifica el nivel de madurez en seguridad de la información en el cual se encuentra la empresa
False	Idempresa	int	True	False	Campo que identifica la empresa en su nivel de madurez Es llave foránea de la tabla empresa
False	Resultado	int	True	False	Campo que almacena el resultado de la madurez de la empresa en seguridad de la información
Name		Type	Columns	Initial Code	
UQ_Tbl_Madurez_Idmadurez		Public	Idmadurez		
PK_Tbl_Madurez		Public	Idmadurez		
FK_Tbl_Madurez_Tbl_Empresa		Public	Idempresa		
FK_Tbl_Madurez_Tbl_NivelMadurez		Public	Idnivel		
Columns		Association			
(Idempresa = Idempresa)		0..* 1	Tbl_Madurez.FK_Tbl_Madurez_Tbl_Empresa Tbl_Empresa.PK_Tbl_Empresa		
(Idnivel = Idnivel)		0..* 1	Tbl_Madurez.FK_Tbl_Madurez_Tbl_NivelMadurez Tbl_NivelMadurez.PK_Tbl_NivelMadurez		

Fuente: Autores

Anexo N. Tabla Tbl_Politicas

Este anexo corresponde al diccionario de datos de Sqlserver, en el cuadro 22 se puede observar la información correspondiente a las políticas en seguridad establecidas en la empresa.

Cuadro 22. Información política de seguridad

PK	Name	Type	Not Null	Unique	Len	Notes
True	Idpoliticas	int	True	True		Campo que identifica las políticas de la empresa
False	Idobjespecifico	int	True	False	0	Campo que identifica los objetivos específicos de la empresa respecto a las políticas en seguridad de la información.
False	Descripción	varchar	True	False	50	Campo que almacena la información general de las políticas en seguridad de la información que tiene establecidas la empresa
Name		Type	Columns			
UQ_Tbl_Politicas_Idpoliticas		Public	Idpoliticas			
PK_Tbl_Politicas		Public	Idpoliticas			
FK_Tbl_Politicas_Tbl_ObjEspecifico		Public	Idobjespecifico			
Columns		Association				
(Idobjespecifico = Idobjespecifico)		0..* 1	Tbl_Politicas.FK_Tbl_Politicas_Tbl_ObjEspecifico Tbl_ObjEspecifico.PK_Tbl_ObjEspecifico			

Fuente: Autores

DISEÑO DE UN SOFTWARE PROTOTIPO QUE PERMITA PARAMETRIZAR UN GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN

Ing. LIANA CAROLINA MONTAÑA CARPINTERO
Ing. JAVIER ALBERTO MONTAÑA CARPINTERO
Ing. DIANA TERESA VALENCIA PEDRAZA

MANUAL TECNICO

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA INGENIERÍA DE SISTEMAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, D.C.
2017

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

MANUAL TECNICO

SOFTWARE PROTOTIPO QUE PERMITA PARAMETRIZAR UN GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN

INTRODUCCIÓN

Pgseg es un software diseñado con el fín de permitir el establecimiento óptimo de un gobierno de seguridad de la información en cualquier tipo de empresa. Para ello cuenta con un sistema modular que permite el ingreso de información actualizada y verídica, esto gracias a la colaboración de los directivos, jefes de área y su personal de apoyo. Pgseg se retroalimenta de información y le permite al oficial de seguridad de la información poder realizar un análisis verás y obtener informes inmediatos que al ser analizados por el experto en seguridad permitirán tomar las medidas adecuadas para minimizar los riesgos a los cuales se exponen los activos críticos de información en las empresas. Al analizar todos estos aspectos en la seguridad de una organización los altos directivos se han dado cuenta que la información es un recurso critico si no el más importante de la empresa y por esto mismo debe tener un tratamiento adecuado como cualquier otro activo de la organización. La seguridad de la información se basa en la disponibilidad, integridad y confidencialidad de los activos de información.

Objetivos del manual acercar al área encargada de TI, en el adecuado procedimiento de instalación del software y configuración de los programas necesarios con el fin de realizar la instalación del prototipo correctamente.

Este manual pretende proporcionar al lector la lógica con la cual se ha diseñado el software prototipo y los componentes tecnológicos sobre los cuales funciona correctamente así como la adecuada instalación del mismo.

Requerimientos de instalación

Para poder instalar la aplicación se requiere de un servidor que tenga instalado y configurado el IIS (Internet Information Services), un servidor que tenga instalado SQL server 2014 y el framework 4.5 Microsoft.NET

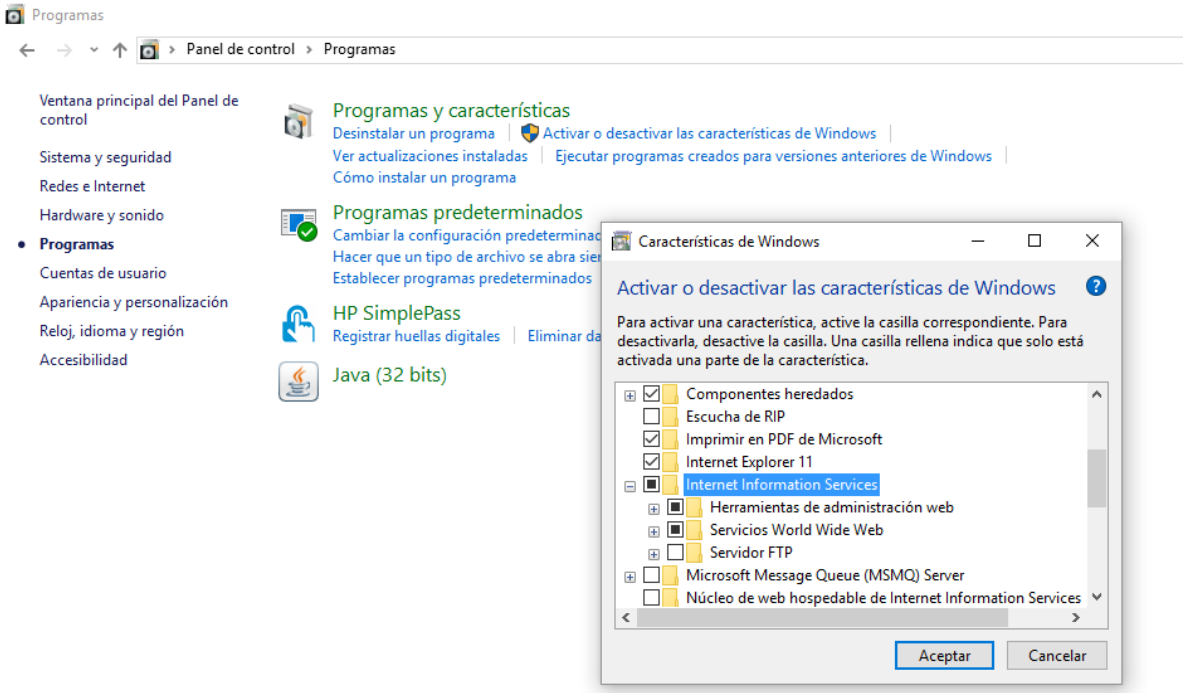
1. CONFIGURACIÓN INTERNET INFORMATION SERVICES

En la figura 1 usted puede observar los pasos para configurar y activar el servidor web en el servidor.

Ir a panel de control
En programas y características
En Activar o desactivar las características de Windows buscar y seleccionar las siguientes opciones:

- Internet Information Services
- Herramientas de administración web
- Servicios Word Wide Web

Figura 1 Activar IIS

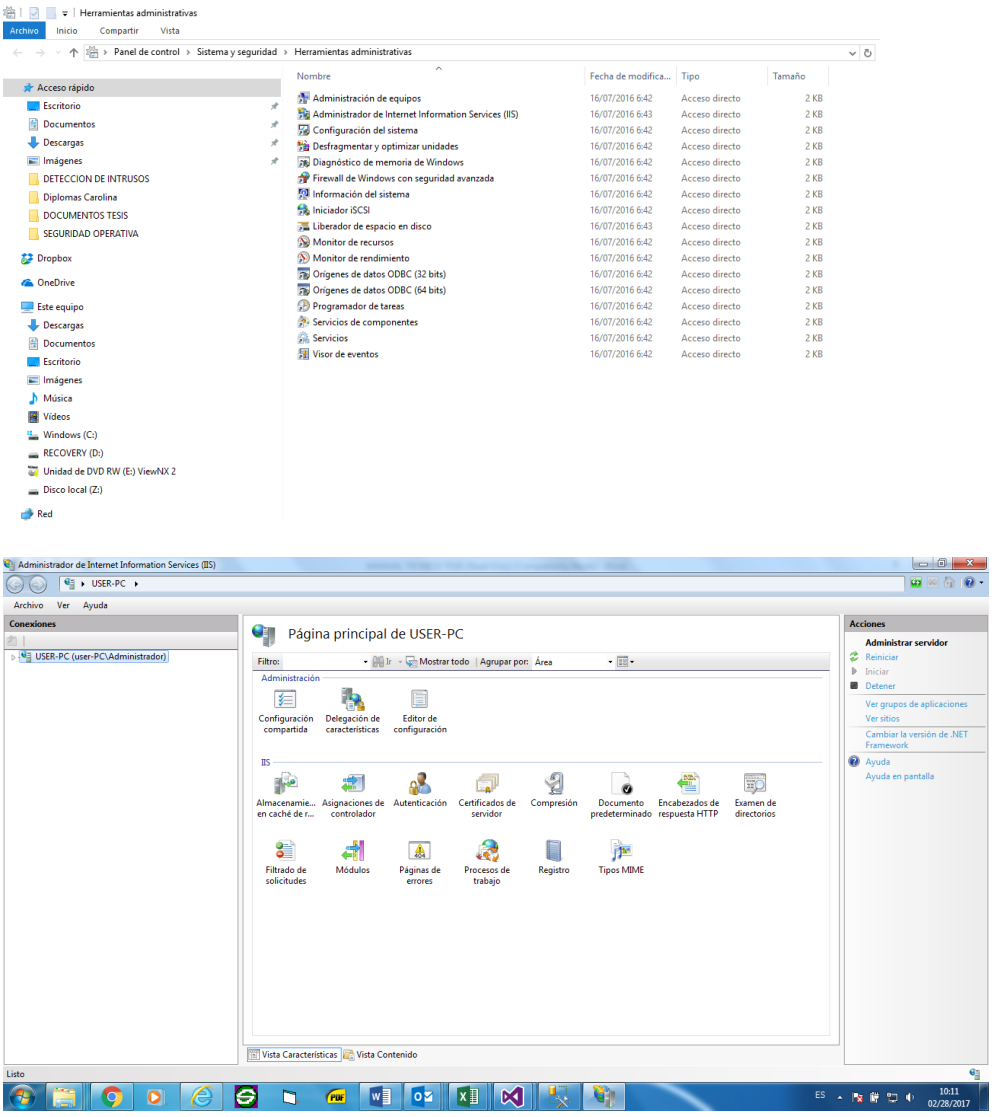


Fuente. Windows

1.1 HERRAMIENTAS ADMINISTRATIVAS

Se debe validar que no vaya a estar bloqueado por un firewall. Una vez instalado IIS debe comprobar que el administrador de internet Information services se encuentre instalado en herramientas administrativas. Una vez rectifique su instalación haga doble clic sobre el administrador de internet Information services tal como se aprecia en la figura 2

Figura 2 Comprobar activación IIS



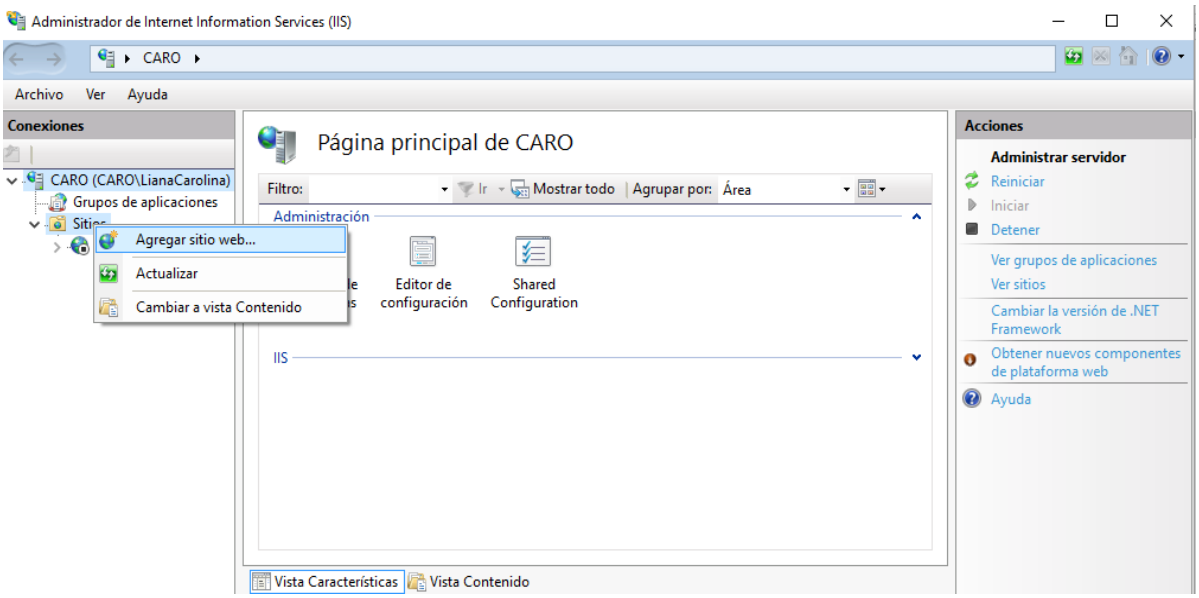
Fuente. Windows

1.2 PUBLICAR APLICACIONES EN IIS

En la entrega se adjunta una carpeta llamada PGSEC, en donde se encuentran los archivos necesarios para poder realizar correctamente la instalación. A continuación se describen los pasos para realizar la instalación en un servidor Windows.

Desde el administrador de Internet Information Services (IIS) Ir a Sitios y con el botón derecho del mouse seleccionar la opción Agregar sitio web. Ver figura 3

Figura 3 Agregar sitio web en IIS

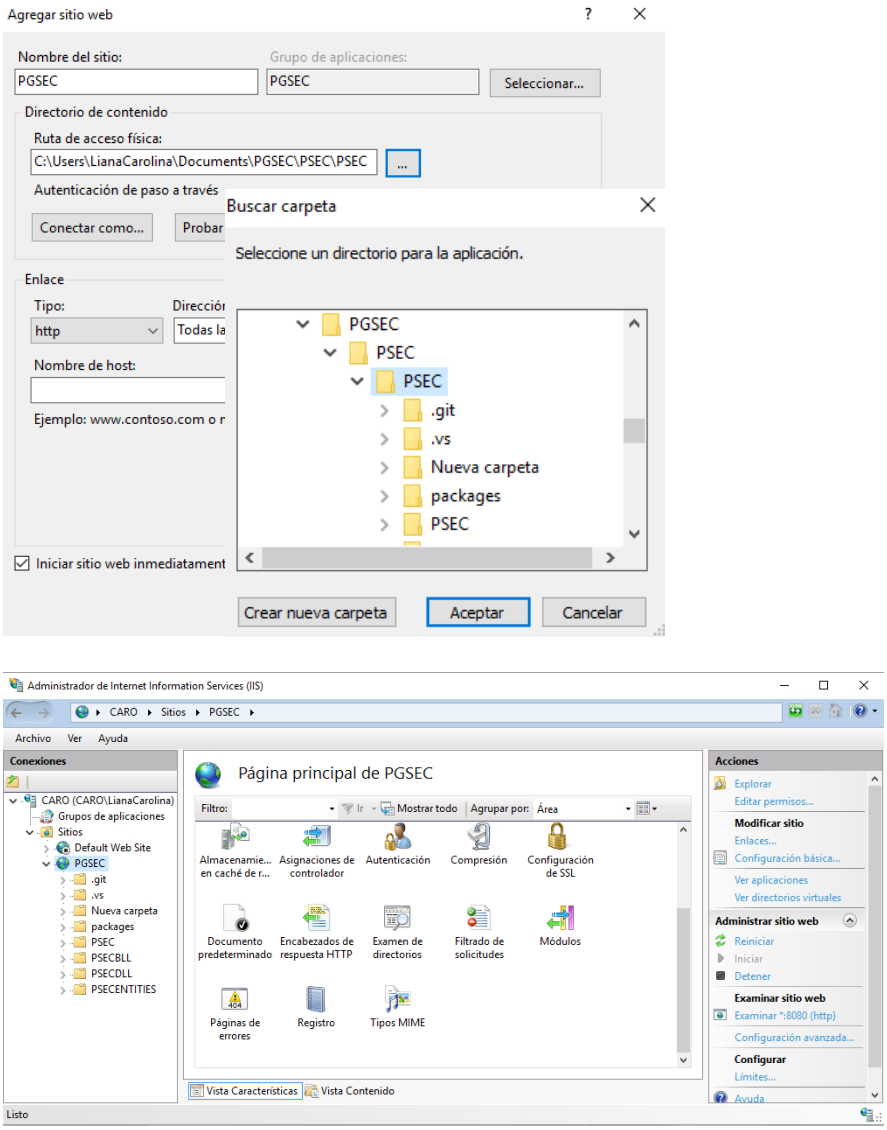


Fuente. Windows

1.3 AGREGAR SITIO WEB EN IIS

En la figura 3 se puede observar la forma adecuada de agregar un nuevo sitio web en IIS para ello debe seleccionar la ruta en la cual se encuentra el código de la aplicación, ver figura 4, comprobación de la página PGSEC.

Figura 4 Agregar sitio web

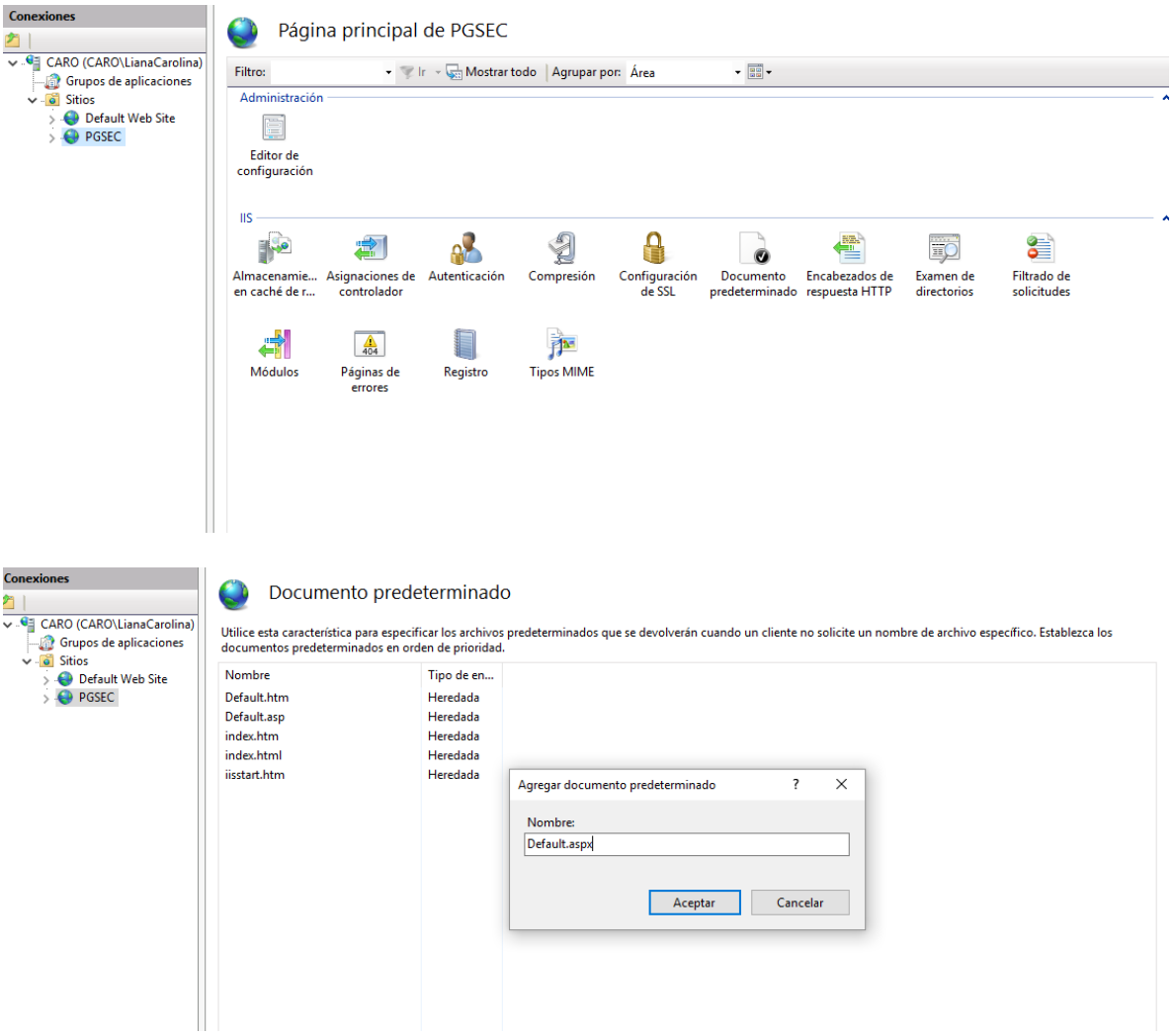


Fuente. Windows

1.4 PÁGINA DEFAULT.ASPX

Es muy importante establecer el documento predeterminado con la página default.aspx tal como se puede observar en la figura 5

Figura 5 Configuración del documento predeterminado en IIS

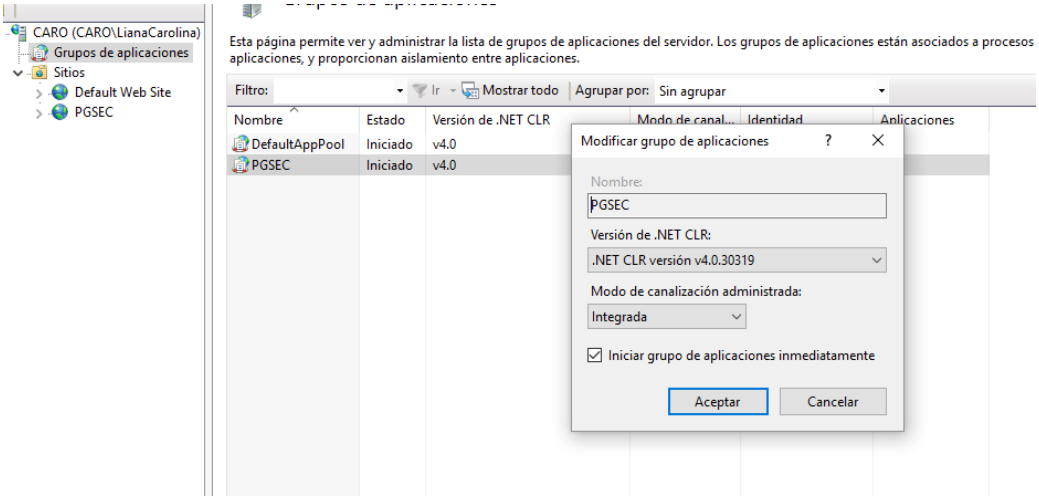


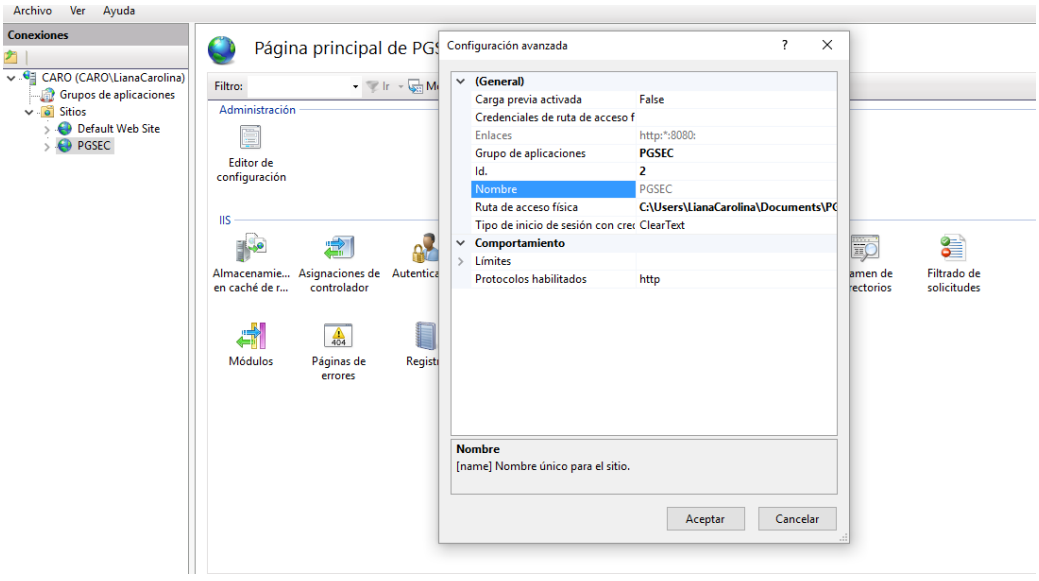
Fuente. autores

1.5 VERSION DEL FRAMEWORK

En la figura 6 se observa como establecer el pool de aplicaciones con la versión del Framework 4.

Figura 6 Version framework



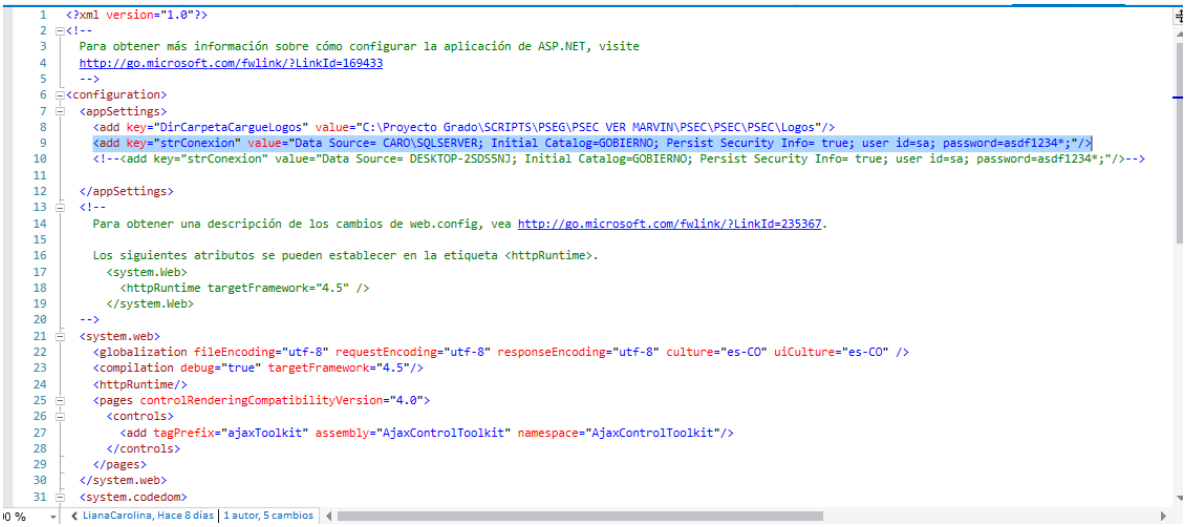


Fuente. Windows

1.6 ACTUALIZAR ARCHIVO WEB.CONFIG

Se debe actualizar el archivo web.config, con la cadena de conexión correspondiente con la dirección del servidor de base de datos tal y como se observa en la siguiente figura 7:

Figura 7 Archivo web.config



Fuente. Windows

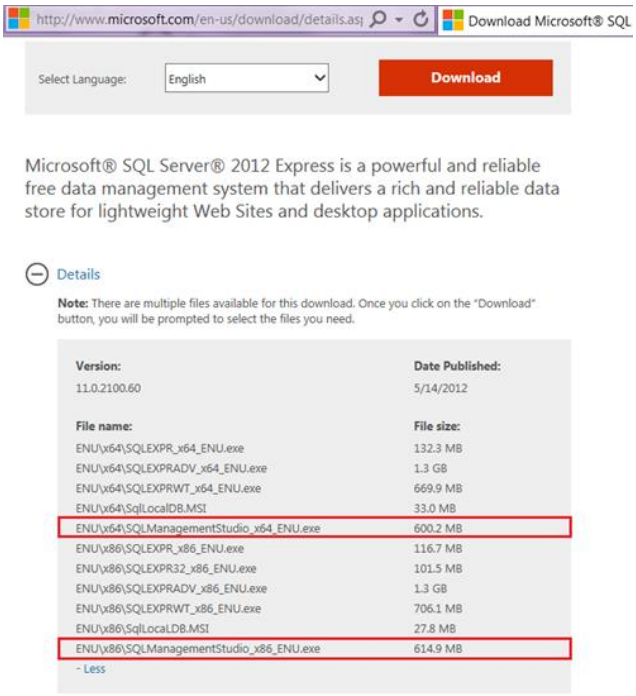
2. INSTALACIÓN BASE DE DATOS SQL SERVER

Los pasos para instalar SQL server management studio 2014 se encuentran en el siguiente enlace. http://www.sqlshack.com/es/sql-server-management-studio-una-guia-de-instalacion-paso-a-paso/ siga las instrucciones paso a paso. Toda la información gráfica y de contenido fue obtenida directamente de esta página.

2.1 DESCARGAR ARCHIVOS DE INSTALACIÓN SQL SERVER MANAGMENT

Primero que nada usted necesita descargar los archivos de instalación de SQL Server Management Studio (SQLManagementStudio_x64_ENU.exe / SQLManagementStudio_x86_ENU.exe) desde la página de descargas de SQL Server dependiendo del tipo de su servidor (x64, x86), y mantenerlos en una carpeta separada[1]. Ver figura 8.

Figura 8 Descargar archivos de instalación sql server



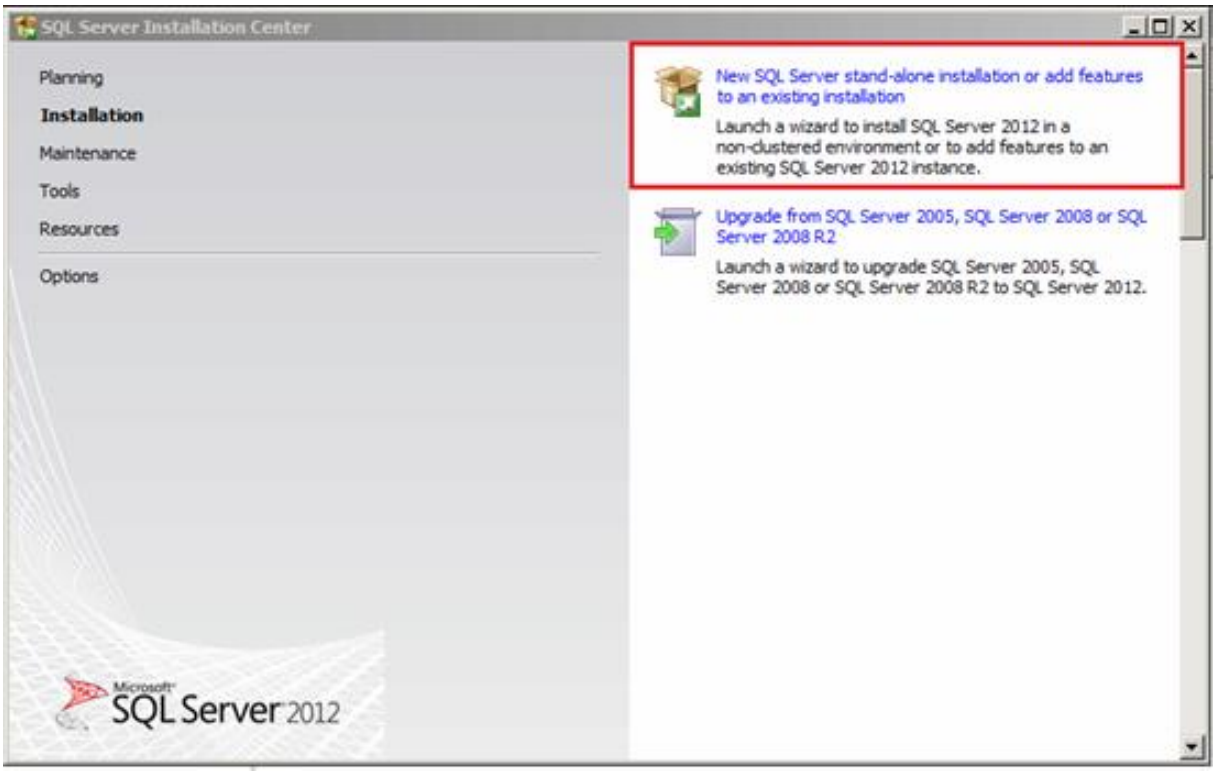
Fuente. Windows

[1] http://www.sqlshack.com/es/sql-server-management-studio-una-guia-de-instalacion-paso-a-paso/

2.2 INSTALACIÓN SQL SERVER INSTALLATION CENTER

Paso 1: Una vez que ha descargado el archivo respectivo para su tipo de servidor, usted necesita ejecutarlo. Eso lo llevará a la primera pantalla llamada SQL Server Installation Center, como se muestra a continuación. Esta es la pantalla primaria de instalación de SQL Server. Otras instalaciones de herramientas de SQL Server pueden ser lanzadas desde aquí también. Una vez que esté en esta pantalla, usted necesita seleccionar "New SQL Server stand-alone installation or add features to an existing installation" para proceder con la instalación[2]. Ver figura 9

Figura 9 Instalación sql server

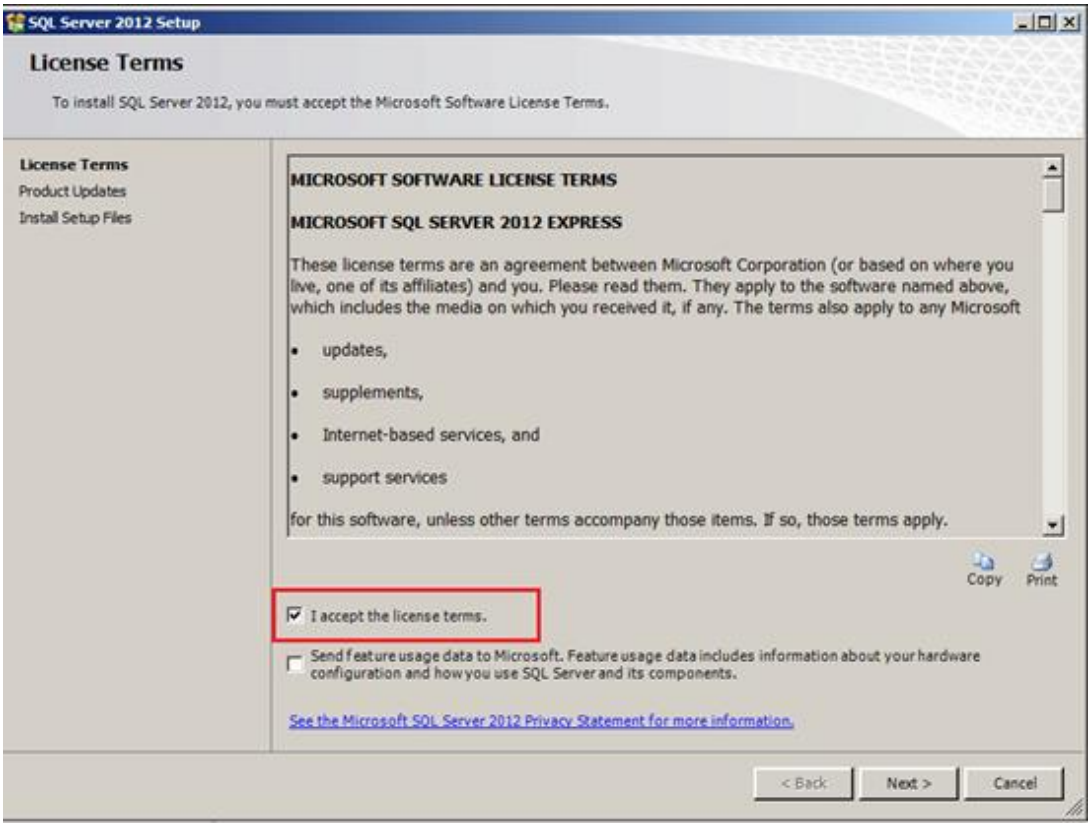


Fuente. Windows

Paso 2: Una vez que seleccione la opción "New SQL Server stand-alone installation or add features to an existing installation", tal opción seleccionará las reglas de configuración (pre-requisitos) en el servidor y lo llevará a la pantalla de **términos de licencia**. Los términos de licencia deben ser leídos y aceptados como los términos de cualquier otra aplicación. Por favor note que usted debe pasar las reglas de configuración para proceder con la instalación.[3] Ver figura 10

[2] http://www.sqlshack.com/es/sql-server-management-studio-una-guia-de-instalacion-paso-a-paso/
[3] http://www.sqlshack.com/es/sql-server-management-studio-una-guia-de-instalacion-paso-a-paso/

Figura 10 Instalación sql server

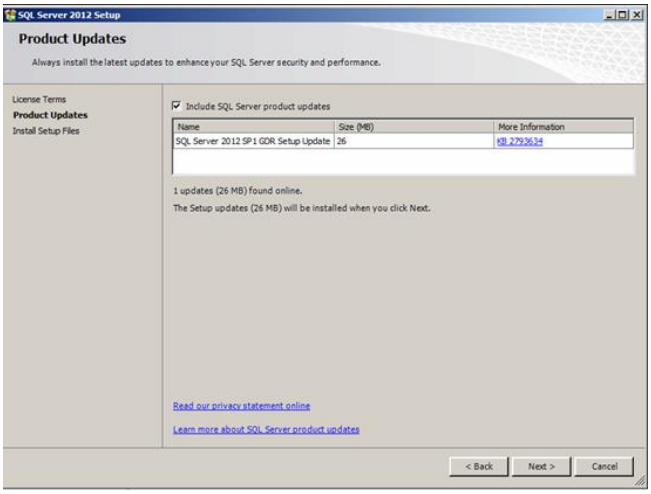


Fuente. Windows

Paso 3: Una vez que acepta los términos de licencia, es tiempo de escanear todas las actualizaciones disponibles para el producto. Las actualizaciones requeridas, el tamaño y los detalles serán mostrados. De todas maneras, si usted necesita más detalles, usted puede seleccionar **More Information**, lo cual lo llevará a la página de soporte, donde usted encontrará todos los detalles relacionados a las actualizaciones. Usted puede ignorar estas actualizaciones deseleccionando la opción '**Include SQL Server product updates**' en este punto.[4] Ver figura 11

[4] http://www.sqlshack.com/es/sql-server-management-studio-una-guia-de-instalacion-paso-a-paso/

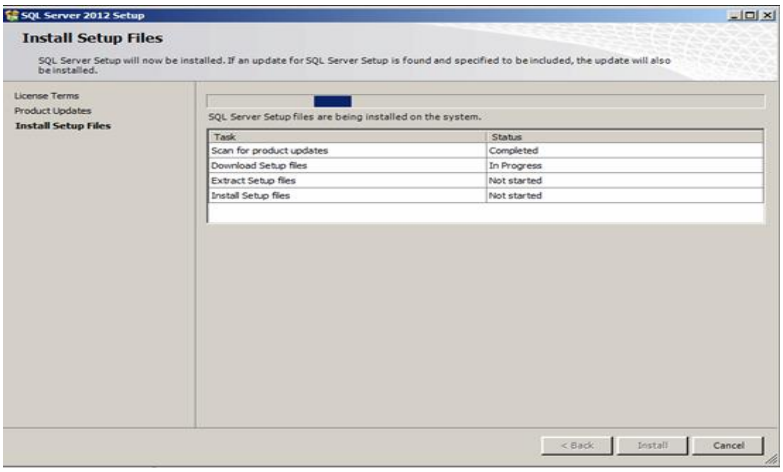
Figura 11 Instalación sql server



Fuente. Windows

Paso 4: El siguiente paso es Install Setup Files, donde la configuración de SQL Server Management Studio (SSMS) descargará e instalará todos los archivos de configuración necesarios para su servidor.[5] Ver figura 12

Figura 12 Instalación sql server



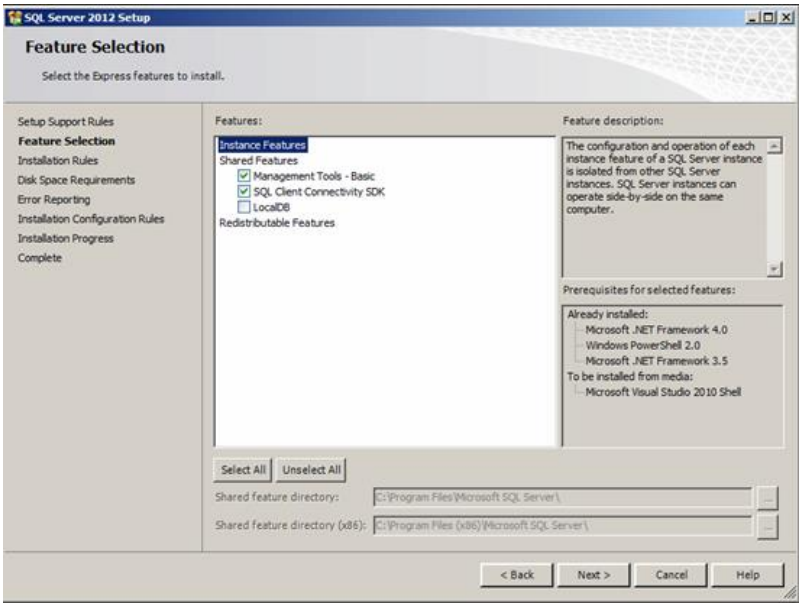
Fuente. Windows

Paso 5: Una vez que la configuración de SQL Server Management Studio (SSMS) está termina la instalación de los archivos de configuración, se verifican las reglas de soporte de configuración para proceder. Luego lo envía a la pantalla de

[5] http://www.sqlshack.com/es/sql-server-management-studio-una-guia-de-instalacion-paso-a-paso/

selección de características. Esta es una pantalla exhaustiva que ha detallado información acerca de cada característica. Para correr la instalación de SQL Server Management Studio (SSMS), se selecciona **Management Tools** por defecto, así que usted no necesita seleccionar nada aquí. Adicionalmente usted puede seleccionar **Management tolos – Basic**. Para obtener más información acerca de esta característica usted puede ver la descripción detallada de la característica en el lado derecho.[6] Ver figura 13.

Figura 13 Sql server instalación

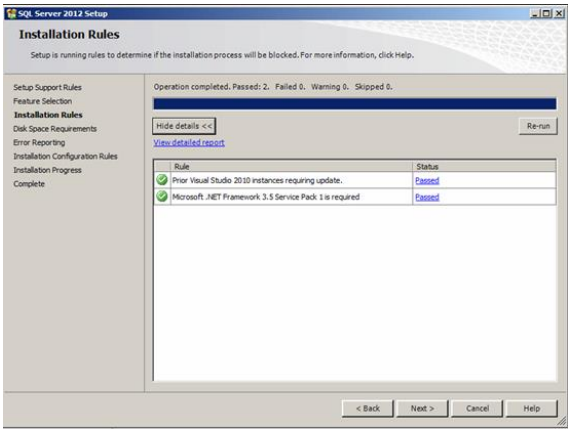


Fuente. Windows

Paso 6: En este paso, SQL Management Studio (SSMS) verificará las reglas de instalación (pre requisito para SSMS). Sólo haga clic en el botón Next para continuar. Ver figura 14

[6] http://www.sqlshack.com/es/sql-server-management-studio-una-guia-de-instalacion-paso-a-paso/

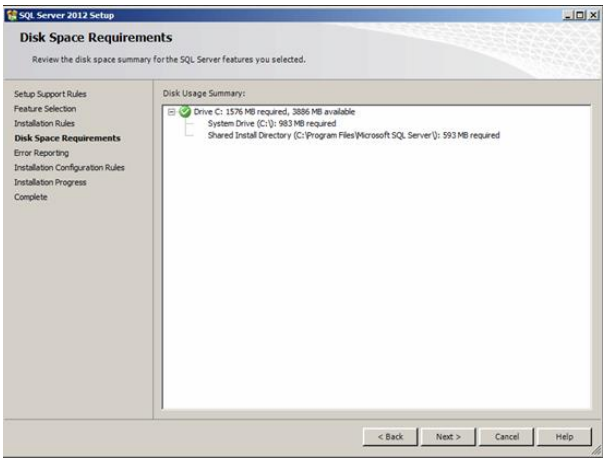
Figura 14 Reglas de instalación sql server



Fuente. Windows

Paso 7: En este paso la configuración de SQL Server Management Studio (SSMS) verificará el espacio del disco. Por favor asegúrese de que tiene suficiente espacio de disco disponible. No tener suficiente espacio de disco puede resultar en fallas en la instalación. Haga clic en el botón Next para continuar.[7] Ver figura 15

Figura 15 Instalación sql

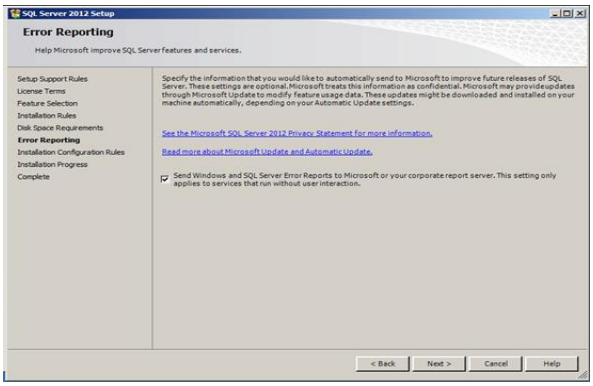


Fuente. Windows

[7] http://www.sqlshack.com/es/sql-server-management-studio-una-guia-de-instalacion-paso-a-paso/

Paso 8: En este paso, usted tiene la oportunidad de decidir si mandar o no notificaciones de error a Microsoft. Esto es altamente recomendado para ayudar a Microsoft a mejorar futuros lanzamientos y para solucionar errores en el lanzamiento existente.[8] Ver figura 16

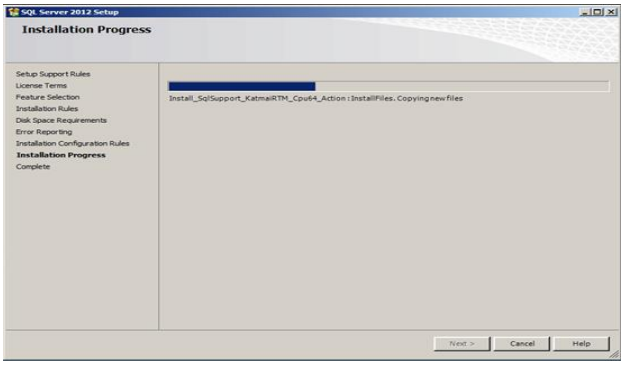
Figura 16 Sql server



Fuente. Windows

Paso 9: Una vez que hace clic en el botón Next, se verificarán las reglas de configuración y si pasaron, el asistente continuará. Este paso tomará tiempo para instalar SQL Server Management Studio. [9]Usted puede sentarse y relajarse. Ver figura 17

Figura 17 Progreso de instalación sql server

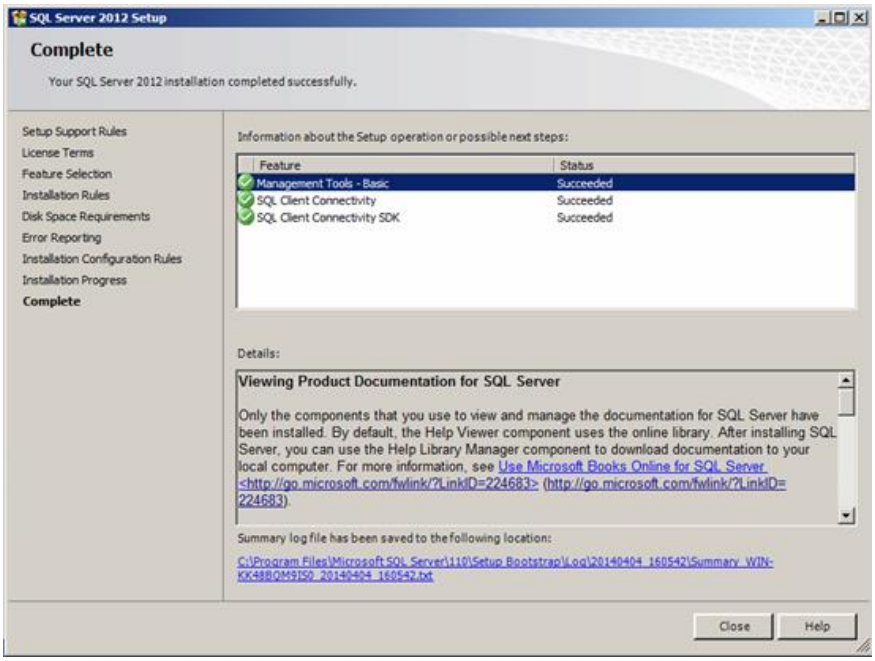


Fuente. Windows

[8] http://www.sqlshack.com/es/sql-server-management-studio-una-guia-de-instalacion-paso-a-paso/
[9] http://www.sqlshack.com/es/sql-server-management-studio-una-guia-de-instalacion-paso-a-paso/

Paso 10: Este paso muestra el estado de instalación de SQL Server Management Studio (SSMS) junto con cada característica, como un resumen. Esta pantalla realmente ayuda a ver qué ha sido instalado y qué no. En el caso de que una de las características no pueda ser instalada, usted puede volver a correr el mismo procedimiento de instalación e instalar esa característica particular.[10] Ver figura 18

Figura 18 Instalación sql server completa

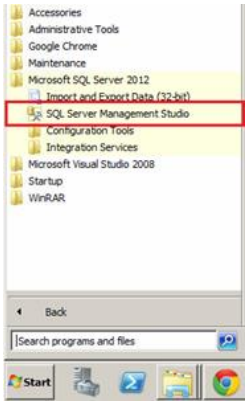


Fuente. Windows

Paso 11: Para verificar si SQL Server Management Studio (SSMS) se ha instalado exitosamente, usted necesita seleccionar el menú de inicio de su servidor y después seleccionar el menú SQL Server 2012. Usted encontrará el enlace a SQL Server Management Studio ahí.[11] Ver figura 19

Figura 19 Comprobación de instalación sql server en el sistema

[10] http://www.sqlshack.com/es/sql-server-management-studio-una-guia-de-instalacion-paso-a-paso/
[11] http://www.sqlshack.com/es/sql-server-management-studio-una-guia-de-instalacion-paso-a-paso/

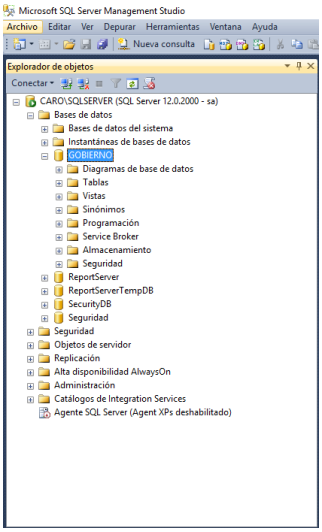


Fuente. Windows

2.3 CREACIÓN DE LA BASE DE DATOS GOBIERNO

Una vez tenga instalado correctamente la versión SQL server management studio 2014. Cree la base Datos GOBIERNO[12]. Ver figura 20

Figura 20 Creación base de datos gobierno



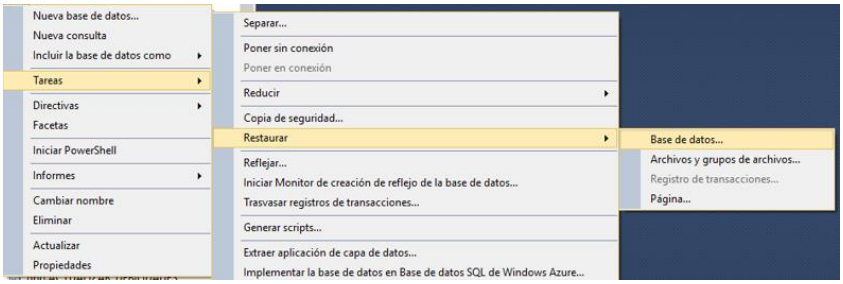
Fuente. Sql

2.3.1 Restaurar base de datos GOBIERNO

[12] http://www.sqlshack.com/es/sql-server-management-studio-una-guia-de-instalacion-paso-a-paso/

Restaure la base de datos del prototipo de software llamada GOBIERNO, el cual se encuentra adjunto al documento, y verifique si la restauración está acorde con la figura 21

Figura 21 Restaurar base de datos gobierno

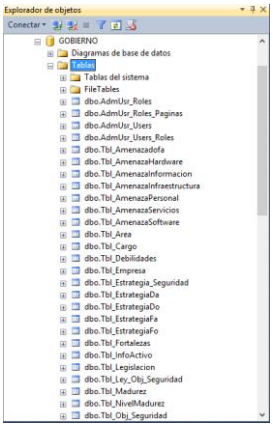


Fuente. Sql

2.3.2 Tablas base de datos GOBIERNO

Una vez haya restaurado correctamente la base de datos rectifique la información que aparece en las tablas de la base de datos GOBIERNO, las cuales se pueden observar en la figura 22.

Figura 22 Tablas de la base de datos gobierno

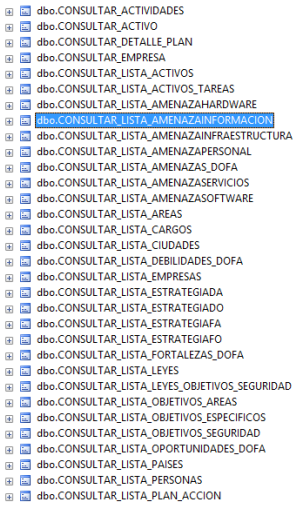


Fuente. Sql

2.3.3 Procedimientos almacenados base de datos GOBIERNO

Rectifique la información que aparece en los procedimientos almacenados de la base de datos GOBIERNO, los cuales se pueden observar en la figura 23

Figura 23 Procedimientos almacenados

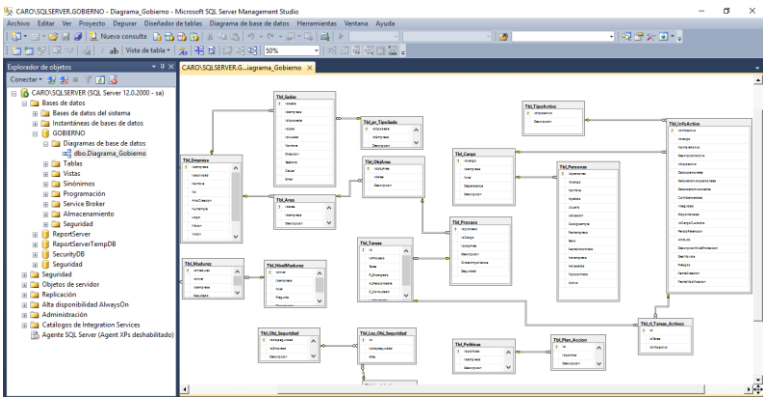


Fuente. Sql

2.3.4 Diagrama relacional base de datos GOBIERNO

En la figura 24 se puede observar el diagrama correspondiente a la base de Datos GOBIERNO.

Figura 24 Diagrama base de datos gobierno

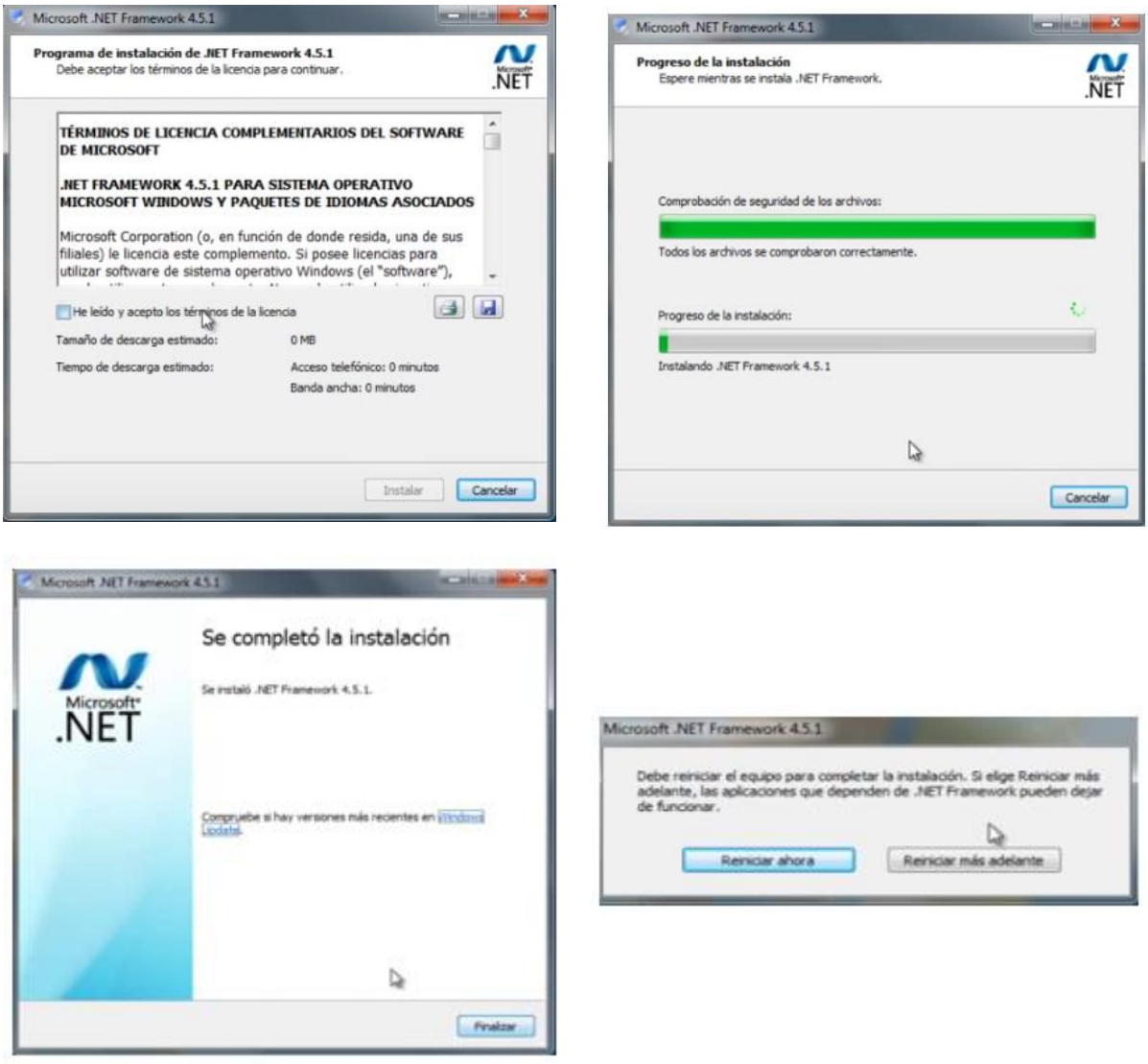


Fuente. Sql

3. INSTALACIÓN MICROSOFT .NET FRAMEWORK 4.5

En la figura 25 se puede observar los procedimientos para la instalación del framework 4.5 de Microsoft.net

Figura 25 Microsoft .net framework

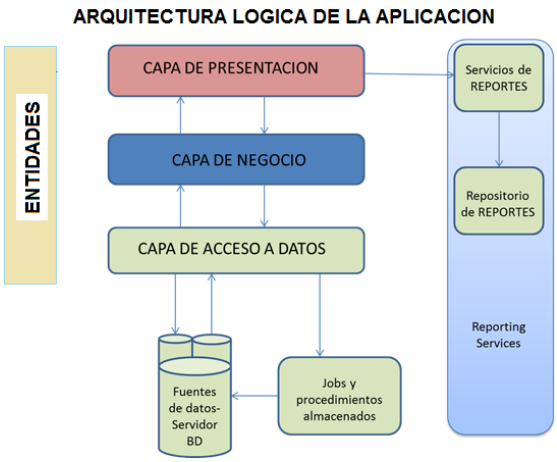


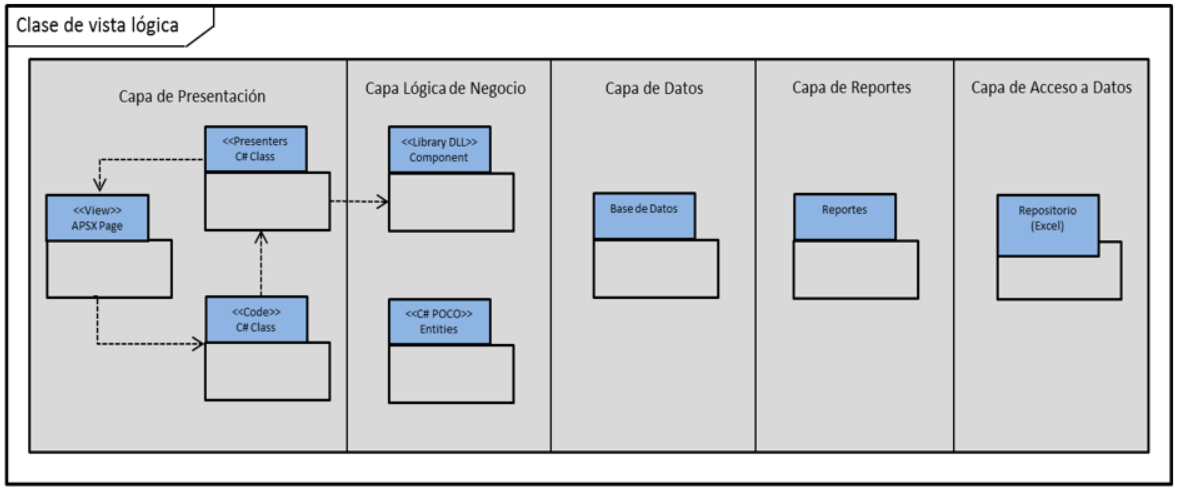
Fuente. Microsoft.net

3.1 PERSPECTIVA LÓGICA APLICACIÓN WEB

La perspectiva lógica es una profundización en el detalle de los elementos de la vista conceptual especialmente de la aplicación PGSEC. Muestra además de las decisiones a nivel de los patrones de software, los módulos funcionales identificados. En la figura 26 se muestra la vista lógica de la aplicación Web.

Figura 26 Arquitectura lógica de la aplicación





Fuente.

Se planteó la utilización de un patrón que permita desacoplar las responsabilidades de procesamiento y presentación de la información. Anticipándonos a la vista de implementación y conociendo que la aplicación Web se desarrollará sobre la plataforma .NET, se recomienda la utilización de una arquitectura de 3 capas.

Entre otros beneficios de la arquitectura multicapa tenemos:

- Mantenibilidad y escalabilidad de los módulos.
- Compartir código entre páginas que requieren los mismos comportamientos.
- Separar la lógica de negocio de la lógica de presentación obteniendo un código más entendible.

Se trata de una aplicación Web multicapa (n-capas) con las capas de Presentación, Negocio y Acceso a Datos. A continuación se describen los elementos arquitectónicamente significativos incluidos en cada una de las capas lógicas:

En la capa de presentación se encuentran los componentes necesarios para el despliegue y captura de información, los cuales permiten al usuario interactuar con el sistema. Esta capa se comunica con la capa de negocio.

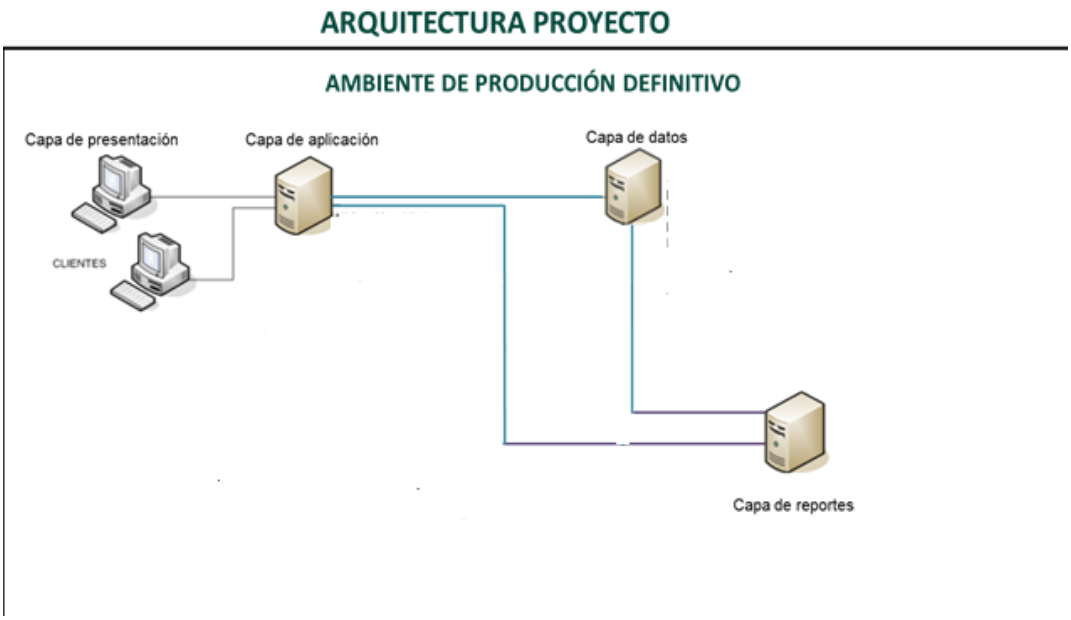
La capa de negocio contiene los componentes y algoritmos que implementan las reglas de negocio, recibe las peticiones de la capa de presentación y se comunica con la capa de datos.

La capa de datos contiene componentes que permite acceder a los datos, recibe las peticiones de la capa de negocio y se comunica con el motor de base de datos.

3.2 PERSPECTIVA DE DESPLIEGUE

La vista física o vista de despliegue muestra cómo los componentes de implementación se ubican en máquinas físicas o virtuales al desplegar la aplicación en producción. Los reportes pueden instalarse directamente en el servidor de base de datos o en otro servidor con SQL server. Como se puede observar en la figura 27.

Figura 27 Perspectiva de despliegue



Fuente. Web

4. PROGRAMACIÓN EN TRES CAPAS

Todo sistema que gestiona datos tendrá una base de datos para guardar esos datos y una interfaz de usuario que será con la que interactúan los usuarios. Además, una parte del sistema se encargará de procesar los datos y gestionar lo que se hace con ellos. La arquitectura en tres capas lo que hace es dividir el sistema en tres partes diferenciadas, de tal forma que cada capa solo se comunique con la inferior[13]

La aplicación se encuentra desarrollada en Visual Studio 2015, realizada utilizando la arquitectura de tres 3 capas.

La capa de presentación contiene las páginas Front End de la aplicación, en ella se encuentran una página maestra (. master) y páginas que utilizan esta maestra (aspx). Estas páginas aspx, contienen un codebehind con extensión .cs en donde se encuentra la lógica de programación de cada página.

Además, se encuentran carpetas como imágenes, css, js (javascript) para la programación del lado del cliente.

En otro proyecto se encuentra la capa de Negocio, en donde se encuentra la lógica de negocio de la aplicación.

En otro proyecto se encuentra la capa de Datos, que es en donde se conecta directamente con la Base de datos.

En otro proyecto se encuentran las entidades referentes al proyecto y con las cuales se instancian los diferentes objetos dentro de la aplicación.

Por último, se realizó una base de datos en SQL Server 2014, la cual contiene las tablas, procedimientos almacenados y funciones requeridas para poder hacer funcionar la aplicación.

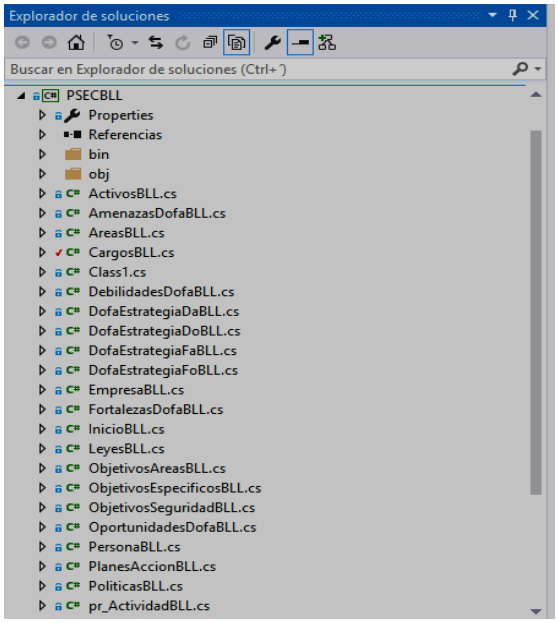
También posee unos reportes con formato rpt que se deben instalar en Reporting services de SQL server.

[13] http://instintobinario.com/arquitectura-en-tres-capas/

4.1 CAPA DE NEGOCIO

En la figura 28 se puede observar las clases creadas para la capa de negocio. En ella se incluye toda la lógica de negocio de la aplicación.

Figura 28 Clases de la capa de Negocio

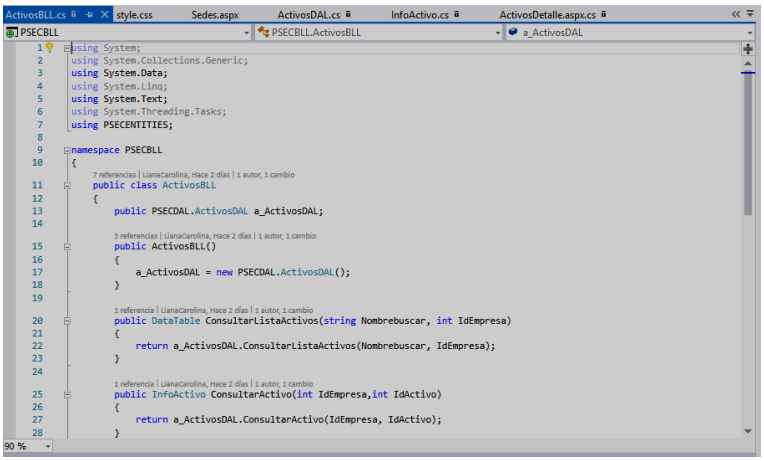


Fuente: Autores

4.1.1 Programación capa de negocio

En la figura 29 se puede observar una parte del código de programación generado para la capa de negocio.

Figura 29 Código capa negocio

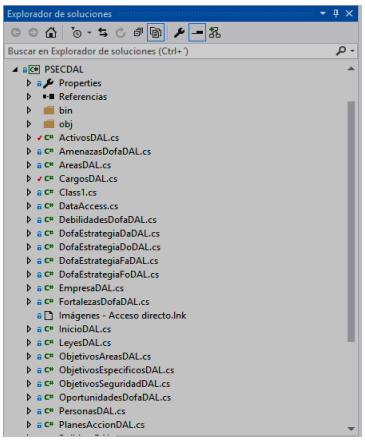


Fuente: Autores

4.2 CAPA DE DATOS

En la figura 30 se puede observar las clases creadas para la capa de datos. Tiene que ver con todo lo referente a la conexión con la base de datos y el llamado a los diferentes procedimientos almacenados.

Figura 30 Clases de la capa de datos

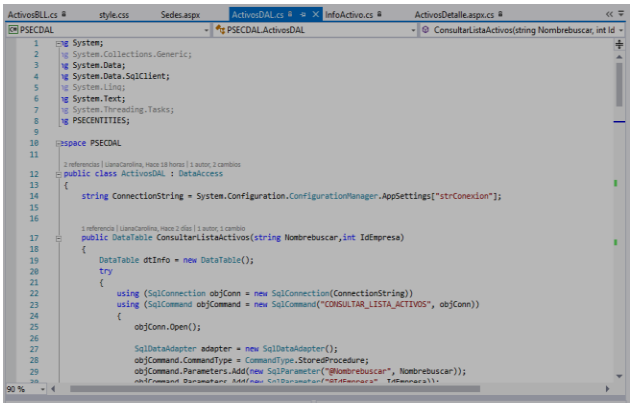


Fuente: Autores

4.2.1 Programación capa de datos

En la figura 31 se puede observar una parte del código de programación generado para la capa de datos.

Figura 31 Código de la capa de datos

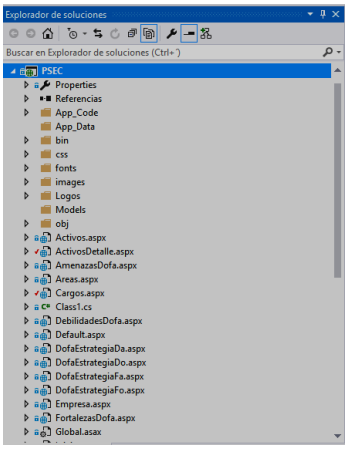


Fuente: Autores

4.3 CAPA DE PRESENTACIÓN

En la figura 32 se puede observar las clases creadas para la capa de presentación. Hace referencia a la parte visual o lo que se le presenta al usuario final de la aplicación conocido también como Front-End.

Figura 32 Clases capa de presentación

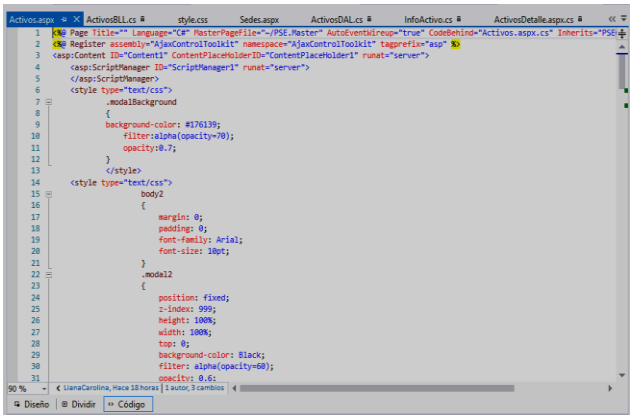


Fuente: Autores

4.3.1 Programación Capa de presentación

En la figura 33 se puede observar una parte del código de programación generado para la capa de presentación.

Figura 33 Código capa presentación

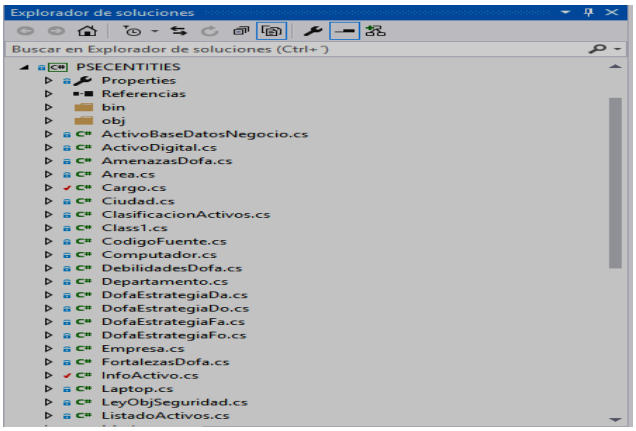


Fuente: Autores

4.4 CAPA ENTIDADES

En la figura 34 se puede observar las clases creadas para la capa de entidades.

Figura 34 Entidades

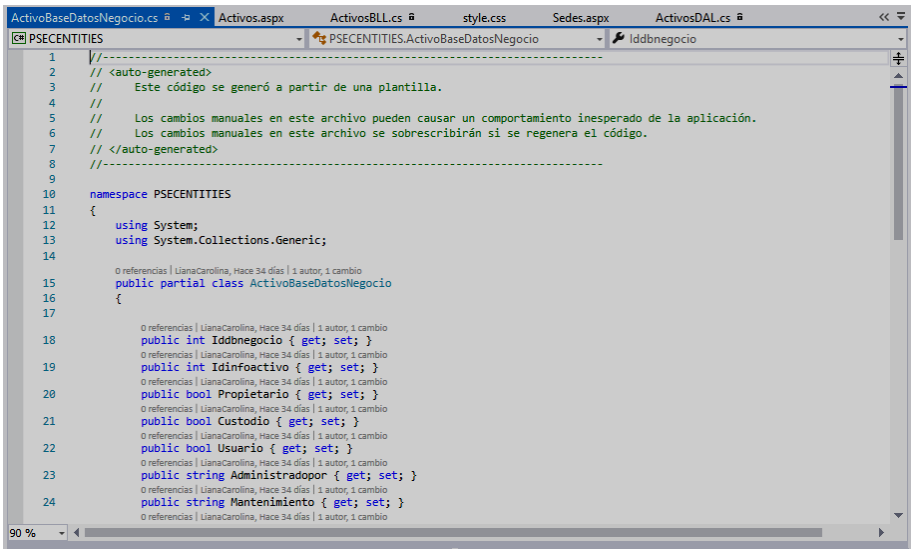


Fuente: Autores

4.4.1 Programación capa de entidades

En la figura 35 se puede observar una parte del código de programación generado para la capa de entidades.

Figura 35 Código entidades

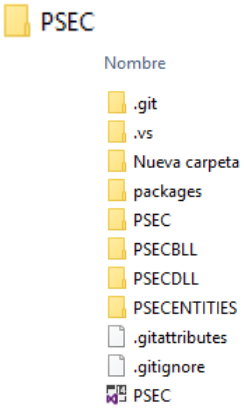


Fuente: Autores

4.4.2 Carpetas que componen el prototipo de software

PSECBLL en esta carpeta se guardan las clases creadas en la capa de negocio, PSECDLL en esta carpeta se guardan las clases creadas para el enlace con la base de datos, PSECENTITIES en esta carpeta se guardan las clases creadas para las entidades . Este contenido se encuentra en la carpeta PSEC y se puede evidenciar en la figura 36

Figura 36 Carpetas prototipo



Fuente: Autores

DISEÑO DE UN SOFTWARE PROTOTIPO QUE PERMITA PARAMETRIZAR UN GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN

Ing. LIANA CAROLINA MONTAÑA CARPINTERO
Ing. JAVIER ALBERTO MONTAÑA CARPINTERO
Ing. DIANA TERESA VALENCIA PEDRAZA

MANUAL DE USUARIO

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA INGENIERÍA DE SISTEMAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, D.C.
2017

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

MANUAL DE USUARIO

SOFTWARE PROTOTIPO QUE PERMITA PARAMETRIZAR UN GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN

INTRODUCCIÓN

Pgseg es un software diseñado con el fín de permitir el establecimiento óptimo de un gobierno de seguridad de la información en cualquier tipo de empresa. Para ello cuenta con un sistema modular que permite el ingreso de información actualizada y verídica, esto gracias a la colaboración de los directivos, jefes de área y su personal de apoyo. Pseg se retroalimenta de información y le permite al oficial de seguridad de la información poder realizar un análisis verás y obtener informes inmediatos que al ser analizados por el experto en seguridad permitirán tomar las medidas adecuadas para minimizar los riesgos a los cuales se exponen los activos críticos de información en las empresas. Al analizar todos estos aspectos en la seguridad de una organización los altos directivos se han dado cuenta que la información es un recurso critico si no el más importante de la empresa y por esto mismo debe tener un tratamiento adecuado como cualquier otro activo de la organización. La seguridad de la información se basa en la disponibilidad, integridad y confidencialidad de los activos de información.

En la medida que se vaya madurando la estructura del gobierno de seguridad dentro de la organización se puede ir planificando la inclusión de la inversión del presupuesto para la seguridad y satisfacer los recursos disponibles para las proyecciones de nuevas tecnologías basadas en seguridad todo alineado a la gestión del riesgo los objetivos organizacionales de los altos directivos. Quienes tendrán una nueva manera de ver a la seguridad con un enfoque global que involucra infraestructura, personas y procesos.

Objetivos del manual acercar al usuario en el adecuado manejo de la aplicación diseñada, dar los lineamientos para el reconocimiento de los diferentes formularios y accesos a la aplicación.

1. CREDENCIALES DE INICIO

Para el ingreso a la aplicación se le solicitara un usuario y su respectiva contraseña en la figura 1 se puede observar el formulario credencial de inicio.

Figura 1 Credenciales

Fuente. Autores

2. LISTA DE EMPRESAS

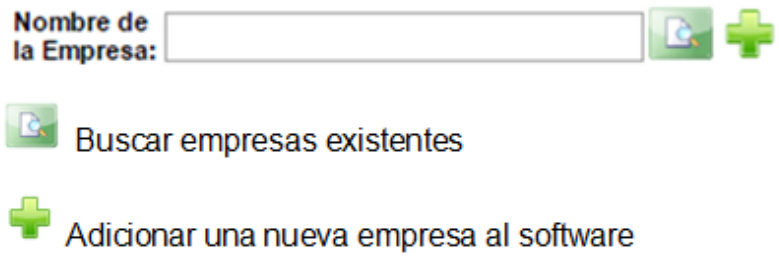
En este formulario el usuario administrador de la aplicación obtiene el ingreso a la información de la empresa. En la figura 2 se puede observar este formulario

Figura 2 Empresas

Fuente. Autores

2.1 COMPONENTES DEL FORMULARIO LISTA EMPRESAS

Figura 3 Lista empresas

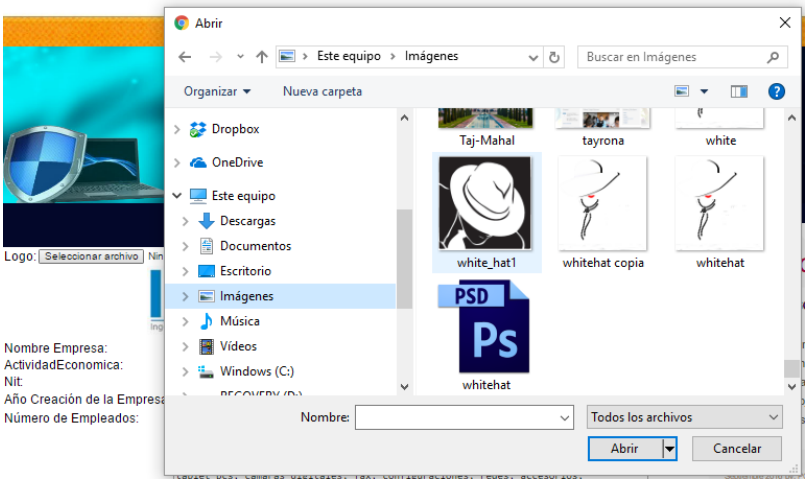


Fuente. Autores

2.1.1 Adicionar una empresa

Cuando se ingresa una nueva empresa el usuario podrá seleccionar su imagen corporativa al hacer clic en el botón seleccionar archivo en el formulario Empresa. En la figura 4 se puede observar una generalidad del formulario.

Figura 4 Adicionar una empresa en la db

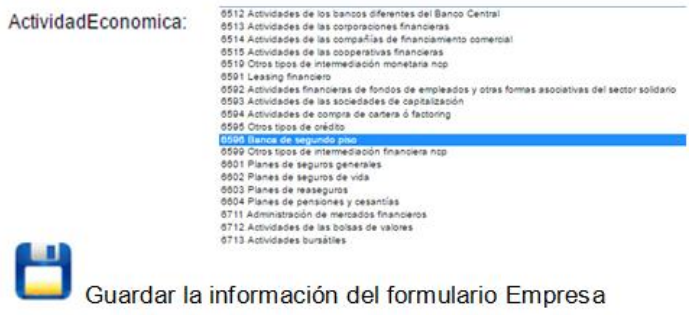


Fuente. Autores

2.1.2 Componentes del formulario lista empresas

En Actividad económica el usuario podrá seleccionar de una lista desplegable las actividades económicas según la cámara de comercio.

Figura 5 Guardar la información formulario lista empresas



Fuente. Autores

2.1.3 Formulario Empresa

En este formulario se solicitará información básica de la empresa se podrá incluir el logo corporativo, nombre de la empresa, seleccionar la actividad económica de una lista desplegable con información actualizada de la cámara de comercio, ingresar el nit de la empresa, el año de creación de la empresa con él se podrá llegar a obtener un acercamiento sobre el nivel de madurez de la empresa en cuanto a sus procesos. Se solicitarán los datos misionales (misión visión y objetivos), Así mismo se indagará acerca de las políticas empresariales que se tienen en seguridad de la información. Datos que serán indispensables para las siguientes fases de identificación y clasificación de los activos estratégicos de información de la empresa, siendo estos la base fundamental del software prototipo planteado. Nombre de la empresa, actividad económica, nit, año de creación de la empresa, misión, visión, objetivo general, políticas empresariales en seguridad de la información. En la figura 6 usted puede observar el formulario empresa.

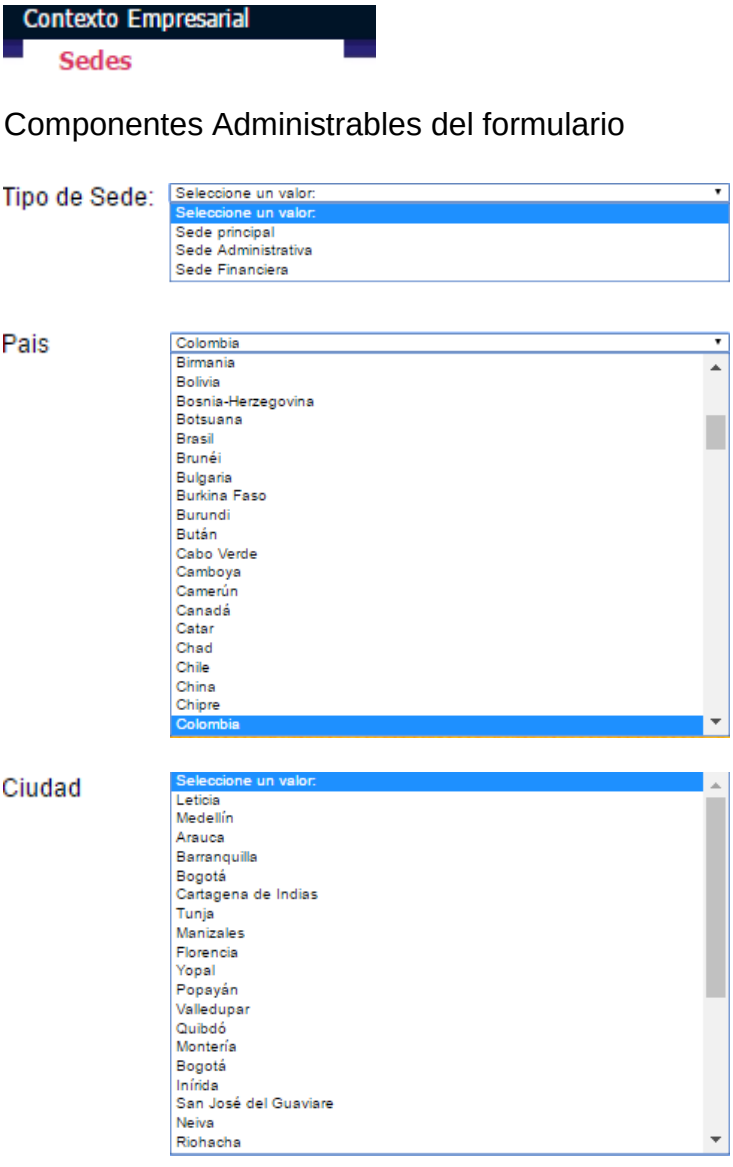
Figura 6 Formulario empresa

Fuente. Autores

3. FORMULARIO SEDES INGRESO INFORMACIÓN

Para ingresar la información en el formulario sedes primero hay que ir al menú Contexto Empresarial y buscar el enlace que dice Sedes, al haga clic sobre este enlace se cargara el formulario correspondiente a la información de las sedes. La figura 7 es una representación funcional del formulario sedes.

Figura 7 Ingreso al formulario



Fuente. Autores

3.1 FORMULARIO SEDES

En este formulario se debe ingresar la información de las sedes de la empresa como tipo de sede, país, ciudad, nombre de la sede, dirección, teléfono, número del móvil y un e-mail de contacto. Una vez se ha ingresado la información de las sedes de la empresa, se mostrará automáticamente en un componente de .net llamado gridview (Muestra los valores de un origen de datos en una tabla donde cada columna representa un campo y cada fila representa un registro. El control GridView permite seleccionar, ordenar y modificar estos elementos aun que para el formulario sedes únicamente se ha habilitado la opción de editar). con este formulario se pretende tener conocimiento de la organización y su contexto empresarial. En la figura 8 se puede observar el formulario sedes.

Figura 8 Formulario sedes

En esta grilla se refleja la información ingresada en el formulario Sedes

Id	Empresa	Tipo Sede	Pais	Ciudad	Nombre	Direccion	Telefono	Celular	Email	Editar
1	ies ltda	Sede principal	Colombia	Bogotá	Sede Galerias	Diagonal 53c No 27 48	2114501	3176724048	iesltda@gmail.com	

Fuente. Autores

5. COMPONENTES FORMULARIO DEBILIDADES DOFA

Para ingresar la información en este formulario debe ir al menú que dice Dofa buscar el enlace que dice debilidades, al hacer clic sobre este enlace se cargara el formulario correspondiente. En la figura 9 puede encontrar una explicación de los iconos encontrados en el formulario.

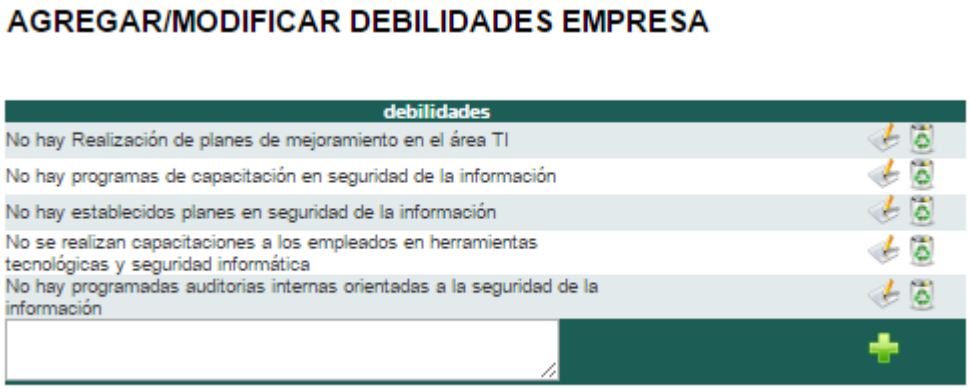
Figura 9 Componentes formulario debilidades dofa

 Edita la información de un registro.

 Elimina un registro de la base de datos y de la grilla.

Adición de un registro en la base de datos.

Presentación de la grilla en el Formulario Debilidades



Fuente. Autores

5.1 Formulario debilidades dofa

El análisis Dofa nos permite identificar la situación actual en la que la empresa se encuentra, las estrategias actuales que la tienen en el mercado y la identificación de las políticas empresariales y aquellos aspectos que se relacionan con la seguridad de la información. En este formulario se debe ingresar la información correspondiente al Dofa en seguridad de la información. En el formulario que se puede apreciar un listado de las posibles debilidades encontradas en materia de

seguridad de la información en la empresa. La figura 10 representa el formulario debilidades

Figura 10 Formulario debilidades dofa

Fuente. Autores

6. COMPONENTES FORMULARIO OPORTUNIDADES DOFA

Para ingresar la información en este formulario debe ir al menú que dice Dofa buscar el enlace que dice oportunidades, al hacer clic sobre este enlace se cargara el formulario correspondiente. En la figura 11 usted puede encontrar una Explicación de los iconos encontrados en el formulario oportunidades dofa.

Figura 11 Formulario oportunidades dofa

 Edita la información de un registro.

 Elimina un registro de la base de datos y de la grilla.

Adición de un registro en la base de datos.

Presentación de la grilla en el Formulario Oportunidades

AGREGAR/MODIFICAR OPORTUNIDADES DOFA EMPRESA

Ley	Oportunidades
	Disposición de infraestructura tecnológica
	Fuentes de financiación propias
	Ética profesional y empresarial
	Cumplimientos jurídicos y legales
Seguridad de la informacion -iso 27001	Implantar un SGSI basados en la Norma ISO 27001:2013
proteccion datos personales-LEY ESTATUTARIA 1581 DE 2012	Acogerse a la legislación que ofrece el decreto de ley Estatutaria 1581 del 2012 en lo que se refiere a protección de datos Personales
Seleccione un Valor	

Fuente. Autores

6.1 FORMULARIO OPORTUNIDADES DOFA

Desarrollo del mercado, vulnerabilidades de la competencia, tendencias de la industria o estilo de vida, desarrollos tecnológicos e innovaciones, influencias globales, nuevos mercados, mercados objetivo, exportación, importación, nuevas propuestas de venta, leyes que se puedan adoptar, tácticas, desarrollo de productos negocios servicios, información e investigación, adopción de nuevas tecnologías, adopción de nuevos procesos.

En este formulario se debe ingresar datos de las oportunidades que tiene la empresa en cuestiones de seguridad de la información. El formulario se diseñó para permitir actualizar las leyes colombianas en temas de seguridad de la información y presentarlas como una opción de oportunidad que la empresa puede llegar a contemplar para fortalecer sus niveles de seguridad. El formulario se puede ver figura 12

Figura 12 Formulario oportunidades dofa

Fuente. Autores

7. COMPONENTES FORMULARIO FORTALEZAS DOFA

Para ingresar la información en este formulario debe ir al menú que dice Dofa buscar el enlace que dice fortalezas, al hacer clic sobre este enlace se cargara el formulario correspondiente. Explicación de los iconos encontrados en el formulario se puede apreciar en la figura 13.

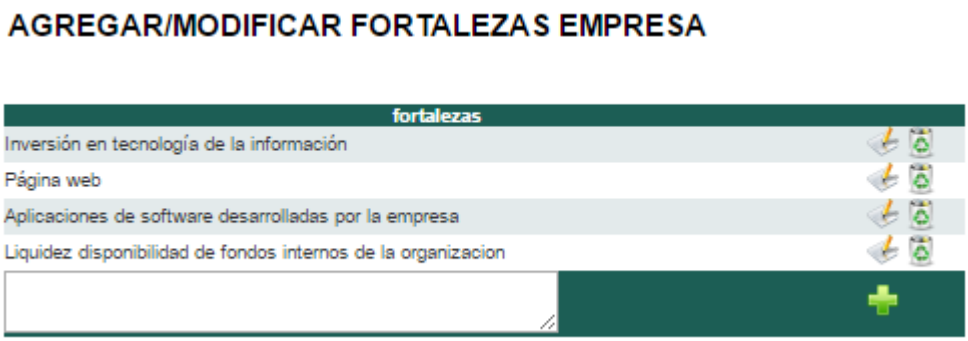
Figura 13 Formulario fortalezas dofa

 Edita la información de un registro.

 Elimina un registro de la base de datos y de la grilla.

Adición de un registro en la base de datos.

Presentación de la grilla en el Formulario Fortalezas

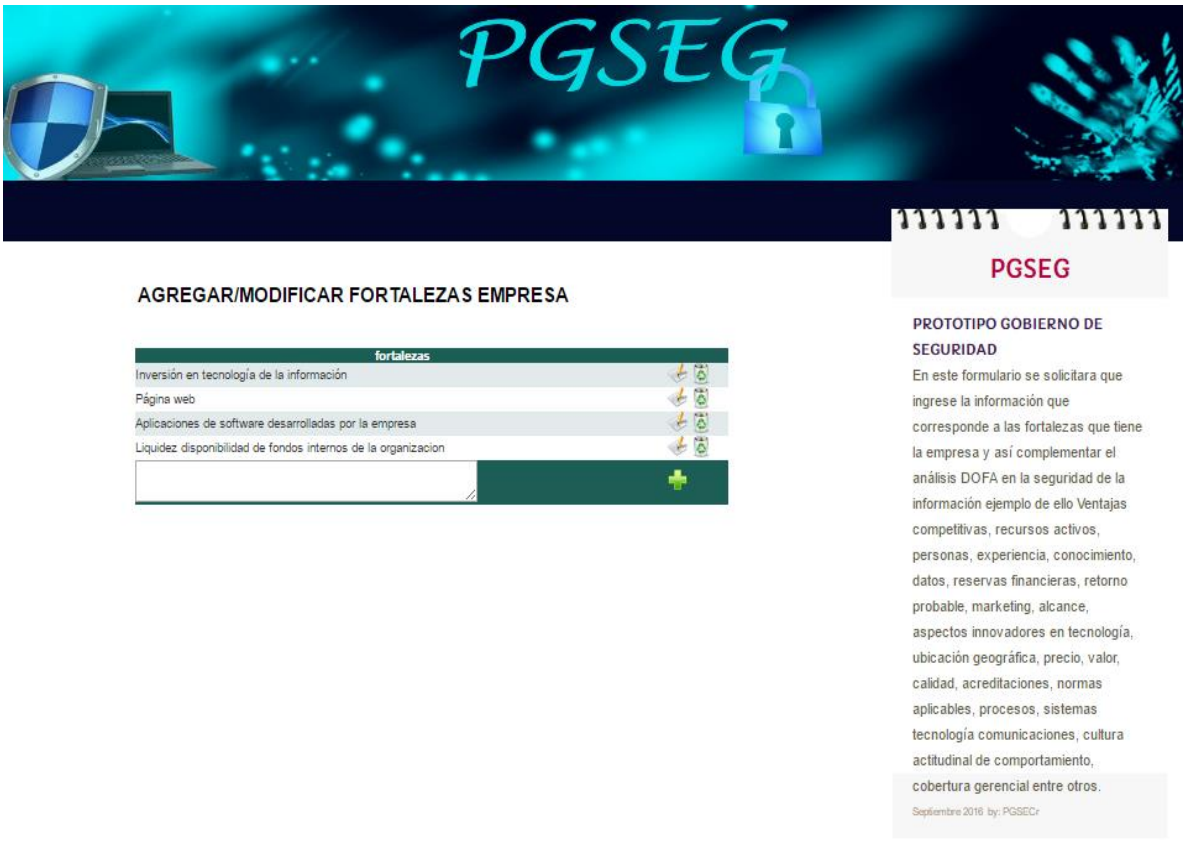


Fuente. Autores

7.1 FORMULARIO FORTALEZAS DOFA

Ventajas competitivas, recursos activos, personas, experiencia, conocimiento, datos, reservas financieras, retorno probable, marketing, alcance, aspectos innovadores en tecnología, ubicación geográfica, precio, valor, calidad, acreditaciones, normas aplicables, procesos, sistemas tecnología comunicaciones, cultura actitudinal de comportamiento, cobertura gerencial entre otros. En este formulario se debe ingresar la información Fortalezas que la empresa tiene a niveles de infraestructura, tecnología y a niveles económicos que la distinguen de otras empresas y que pueden llegar a fortalecer los niveles de seguridad de la información de la empresa.

Figura 14 Formulario fortalezas dofa



Fuente. Autores

8. COMPONENTES FORMULARIO AMENAZAS DOFA:

Para ingresar la información en este formulario debe ir al menú que dice Dofa buscar el enlace que dice amenazas, al hacer clic sobre este enlace se cargara el formulario correspondiente. En la figura 15 encuentra una explicación de los iconos encontrados en el formulario.

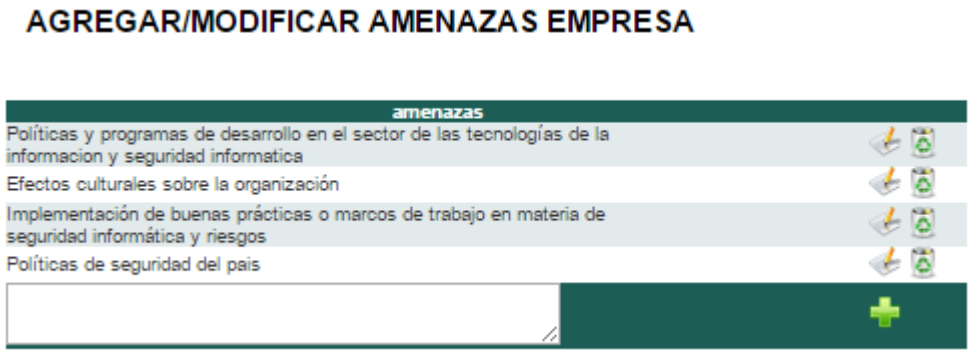
Figura 15 Formulario amenazas dofa

 Edita la información de un registro.

 Elimina un registro de la base de datos y de la grilla.

 Adición de un registro en la base de datos.

Presentación de la grilla en el Formulario Amenazas



Fuente. Autores

8.1 FORMULARIO AMENAZAS DOFA

Efectos políticos, efectos legislativos, desarrollo de ti, intensiones de los competidores, demanda del mercado, nuevas tecnologías, servicios, ideas, amenazas del ambiente exterior. En este formulario se recopilan las posibles amenazas en seguridad de la información que pueden llegar a materializarse en ies ltda si no se llegaran a tomar los controles adecuados, entre los cuales es importante mencionar fortalecer la empresa en las debilidades encontradas en la infraestructura, la tecnología, en los procesos, en el personal y en las políticas generadas en pro de la seguridad de la información. En la figura 16 se puede observar un listado detallado de las amenazas identificas por la empresa.

Figura 16 Formulario amenazas dofa

Fuente. Autores

9. COMPONENTES FORMULARIO ÁREAS

Para ingresar la información en este formulario debe ir al menú que dice Contexto Empresarial buscar el enlace que dice áreas, al hacer clic sobre este enlace se cargará el formulario correspondiente en la figura 17 usted podrá observar la explicación de los iconos encontrados en el formulario

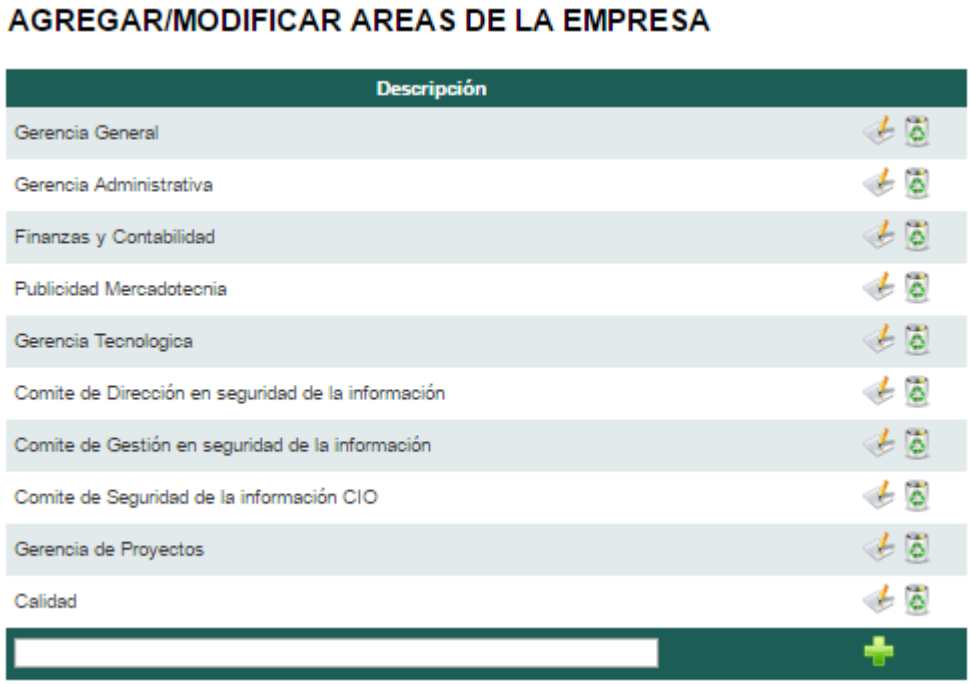
Figura 17 Componentes Formulario áreas

 Edita la información de un registro.

 Elimina un registro de la base de datos y de la grilla.

 Adición de un registro en la base de datos.

Presentación de la grilla en el Formularioa Areas



Fuente. Autores

9.1 FORMULARIO ÁREAS

En este formulario se debe ingresar la información de las áreas que conforman la estructura organizacional de la empresa, así mismo deben quedar estipulados los nombres de los comités designados para el establecimiento del plan de seguridad de la información. En la figura 18 usted podrá apreciar el formulario correspondiente a la información de las áreas de la empresa.

Figura 18 Formulario áreas

Fuente. Autores

10. COMPONENTE FORMULARIO OBJETIVOS DE NEGOCIO

Para ingresar la información en este formulario debe ir al menú que dice Contexto Empresarial buscar el enlace que dice objetivos negocio, al hacer clic sobre este enlace se cargara el formulario correspondiente.

Explicación de los iconos encontrados en el formulario

Figura 19 Componentes formulario objetivos de negocio

 Edita la información de un registro.

 Elimina un registro de la base de datos y de la grilla.

 Adición de un registro en la base de datos.

Presentación de la grilla en el Formularios Objetivos Negocio

AGREGAR/MODIFICAR OBJETIVOS DE NEGOCIO DE LA EMPRESA

Areas	Objetivos
Gerencia General	Dirigir la empresa con responsabilidad y criterio, apoyar y tomar desiciones en las areas del negocio y las concernientes a la seguridad de la empresa
Gerencia Administrativa	Proporcionar servicios administrativos necesarios para la empresa. Promover las acciones requeridas para garantizar el cumplimiento de los Reglamentos, políticas, procedimientos y presupuestos de la Organización.Coordinar la administración del Patrimonio de la Organización.Administrar adecuadamente los recursos y fuentes externas de financiamiento
Finanzas y Contabilidad	Mantener el Presupuesto y Finanzas de la empresa al Dia -Realizar el Pago de Nominas cumplidamente -Tener soporte y control de las cuentas por pagar y cobrar- Informar cualquier cambio en el presupuesto de la empresa- coordinar la atención al cliente
Publicidad Mercadotecnia	Ofrecer al mercado productos nuevos, realizar investigación sobre tendencias en el mercado de productos que pueda ofrecer la empresa sugerir nuevos usos para los productos que oferta, hacer conocer a su target o mercado objetivo cambio de precios, ofertas, descuentos, o simplemente como funciona su producto o servicio.
Gerencia Tecnologica	Mejorar la competitividad de la empresas aumentando el nivel tecnologico mediante la creacion de nuevas tecnologias aplicadas a productos y procesos. desarrollar software de calidad
Comite de Dirección en seguridad de la información	Formado por los Directivos de la empresa, tienen como máxima responsabilidad aprobar las decisiones de alto nivel relativas al sistema de seguridad de la información alineados a los objetivos del negocio
Comite de Gestión en seguridad de la información	Controlará , gestionara, las acciones de la implantación del sistema colaborando con el responsable encargado del comité de seguridad seguridad de la información
Comite de Seguridad de la información CIO	Persona encargada de coordinar las actividades y actuaciones encaminadas a la seguridad de la información en la empresa
Gerencia de Proyectos	Evaluar, planificar, ejecutar, dar seguimiento y control a los proyectos de Ingeniería.
Calidad	Asegurar que la entrega de los productos al cliente cumplan con los estandares de calidad
Seleccione un Valor	

Fuente. Autores

10.1 FORMULARIO ÁREAS

Este formulario ha sido diseñado para el ingreso de los objetivos que el negocio propone en temas de seguridad de la información en la empresa debe incluir los objetivos de los comités designados para el establecimiento y manejo de la seguridad de la información en la empresa.

Figura 20 Formulario áreas

Fuente. Autores

11. COMPONENTES FORMULARIO PROCESOS

Para ingresar la información en este formulario debe ir al menú que dice Contexto Empresarial buscar el enlace que dice procesos, al hacer clic sobre este enlace se cargara el formulario correspondiente. En la figura 21 encuentra una breve explicación de los iconos en el formulario procesos

Figura 21 Componentes formulario procesos

 Edita la información de un registro.

 Elimina un registro de la base de datos y de la grilla.

 Adición de un registro en la base de datos.

Presentación de la grilla en el Formularios Procesos

AGREGAR/MODIFICAR PROCESOS POR OBJETIVOS DE NEGOCIO DE LA EMPRESA

Objetivos	Cargos	Procesos	Orden Importancia	Es politica?
Dirigir la empresa con responsabilidad y criterio, apoyar y tomar desiciones en las areas del negocio y las concernientes a la seguridad de la empresa	Gerente General	Realizar capacitaciones con los Jefes de Departamento y todo el personal.	1	Si
Mejorar la competitividad de la empresas aumentando el nivel tecnologico mediante la creacion de nuevas tecnologias aplicadas a productos y procesos. desarrollar software de calidad	Gerencia Tecnologica	Proceso de Autorización de instalación de hardware o software en los equipos de computo de la empresa	1	Si
Proporcionar servicios administrativos necesarios para la empresa. Promover las acciones requeridas para garantizar el cumplimiento de los Reglamentos, políticas, procedimientos y presupuestos de la Organización.Coordinar la administración del Patrimonio de la Organización.Administrar adecuadamente los recursos y fuentes externas de financiamiento	Gerente Administrativo	Adecuación de espacio físico; energía eléctrica; aire acondicionado; protección contra incendios entre otros orientados a la seguridad de los activos de información	1	Si
Mejorar la competitividad de la empresas aumentando el nivel tecnologico mediante la creacion de nuevas tecnologias aplicadas a productos y procesos. desarrollar software de calidad	Gerencia Tecnologica	Proceso de Monitoreo de accesos lógicos a bases de datos y aplicaciones	1	Si
Dirigir la empresa con responsabilidad y criterio, apoyar y tomar desiciones en las areas del negocio y las concernientes a la seguridad de la empresa	Comite de gestión en seguridad de la información	Definir y documentar los roles yresponsabilidades de los empleados,contratistas y usuarios de terceras partespor la seguridad, de acuerdo con la políticade seguridad de la información de laorganización	1	Si
Dirigir la empresa con responsabilidad y criterio, apoyar y tomar desiciones en las areas del negocio y las concernientes a la seguridad de la empresa	Comité de dirección en seguridad de la informacion	Identificar y revisar con regularidad losrequisitos de confidencialidad o los acuerdos deno-divulgación que reflejan las necesidades dela organización para la protección de lainformación	1	Si
Proporcionar servicios administrativos necesarios para la empresa. Promover las acciones requeridas para garantizar el cumplimiento de los Reglamentos, políticas, procedimientos y presupuestos de la Organización.Coordinar la administración del Patrimonio de la Organización.Administrar adecuadamente los recursos y fuentes externas de financiamiento	CIO en seguridad de la Información	Coordinar la realización de Capacitaciones en seguridad de la información a todo el personal de la empresa incluyendo contratistas y personal de apoyo	1	Si
Seleccione un Valor	Seleccione un Valor			No

1 2

Fuente. Autores

11.1 FORMULARIO PROCESOS

En este formulario se debe ingresar la información de los procesos que la empresa propone en temas relacionados con la seguridad de la información y su orden de importancia.

Figura 22 Formulario procesos

Fuente. Autores

12. COMPONENTES FORMULARIO CARGOS

Para ingresar la información en este formulario debe ir al menú que dice Contexto Empresarial buscar el enlace que dice cargos, al hacer clic sobre este enlace se cargara el formulario correspondiente. La explicación de los iconos encontrados en el formulario se puede ver en la figura 23.

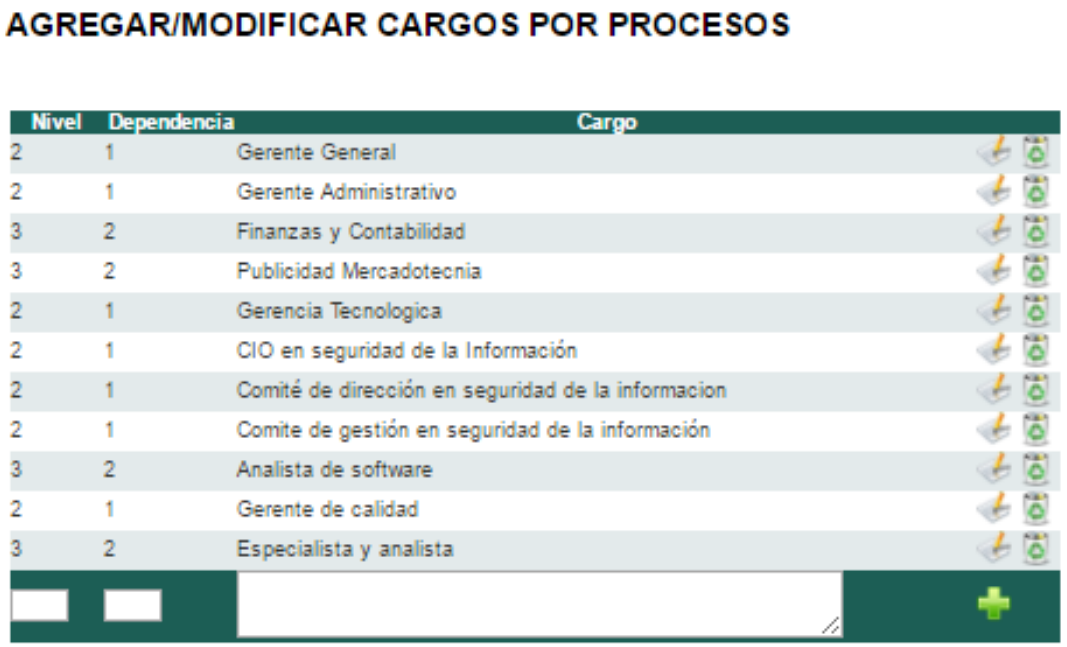
Figura 23 Componentes formulario cargos

 Edita la información de un registro.

 Elimina un registro de la base de datos y de la grilla.

 Adición de un registro en la base de datos.

Presentación de la grilla en el Formularios Cargos



Fuente. Autores

12.1 FORMULARIO CARGOS

En este formulario se debe ingresar la información de los procesos de la empresa representado en el nivel de importancia la dependencia a la cual corresponde y el cargo asignado.

Figura 24 Formulario cargos

Fuente. Autores

13. COMPONENTES FORMULARIO PERSONAS

Para ingresar la información en este formulario debe ir al menú que dice Contexto Empresarial buscar el enlace que dice personas, al hacer clic sobre este enlace se cargara el formulario correspondiente. En la figura 25 se ve una explicación de los iconos encontrados en el formulario

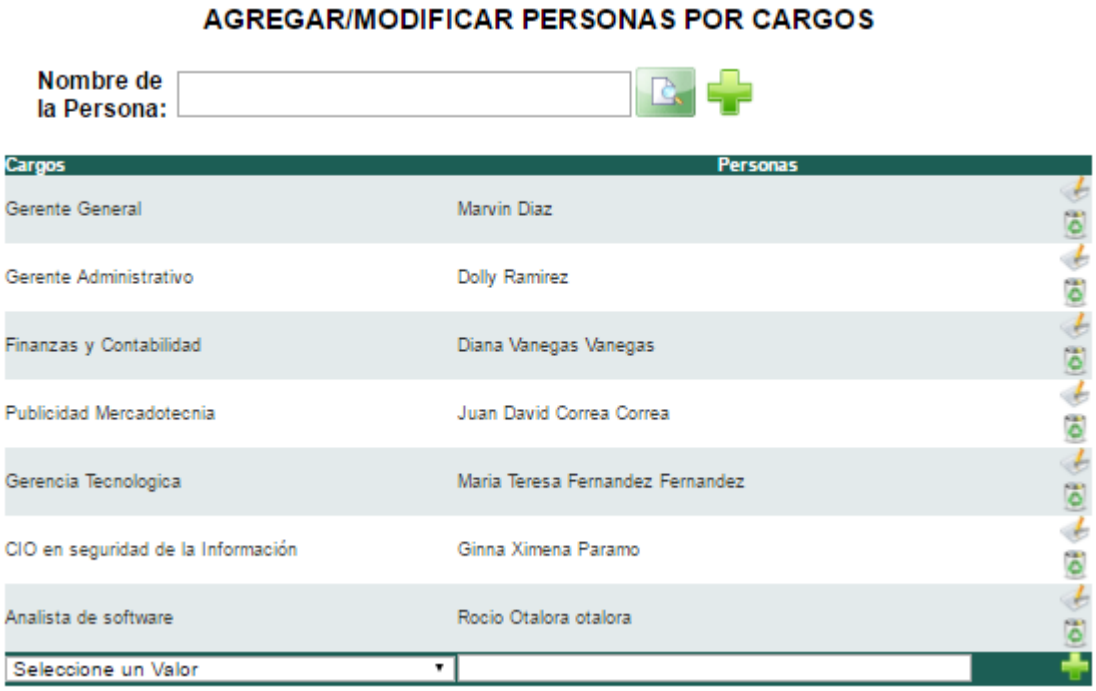
Figura 25 Componentes formularios personas

 Edita la información de un registro.

 Elimina un registro de la base de datos y de la grilla.

 Adición de un registro en la base de datos.

Presentación de la grilla en el Formularios Personas



Fuente. Autores

13.1 FORMULARIO PERSONAS

En este formulario se debe ingresar la información correspondiente a la identificación de las personas que van a participar y tendrán a su cargo labores y funciones orientadas en los temas relacionados con la seguridad de la información de la empresa en el formulario al lado izquierdo se puede encontrar una guía de como completar la información solicitada para la identificación de las personas. Véase la figura 26

Figura 26 Formulario personas

Fuente. Autores

14. COMPONENTES FORMULARIO LISTA ACTIVOS

Para ingresar la información en este formulario debe ir al menú que dice Contexto Empresarial buscar el enlace que dice activos, al hacer clic sobre este enlace se cargara el formulario correspondiente. La explicación de los iconos encontrados en el formulario se puede observar en la figura 27.

Figura 27 Componentes formulario lista activos

 Edita la información de un registro.

 Elimina un registro de la base de datos y de la grilla.

 Permite ingresar a la grilla un nuevo registro.

Busqueda de los activos de información

Presentación de la grilla en el Formularios Lista Activos

En esta grilla se mostrarán una serie de registros que representa los activos identificados como críticos en los procesos de la empresa y que deben ser protegidos de una forma adecuada.

Fuente. Autores

14.1 FORMULARIO LISTA DE ACTIVOS.

En este formulario se debe ingresar la información de la lista de los activos críticos de información, para ello se debe asignar una persona responsable la cual será la encargada de salvaguardar la información de los activos críticos de información en la empresa.

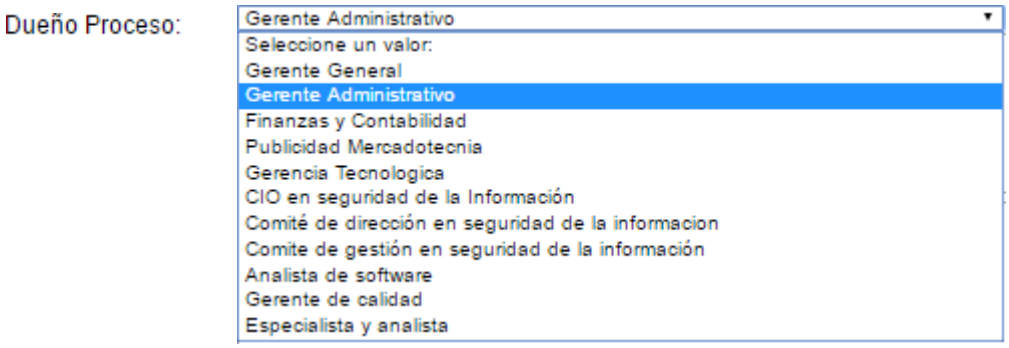
Figura 28 Formulario lista de activos

Fuente. Autores

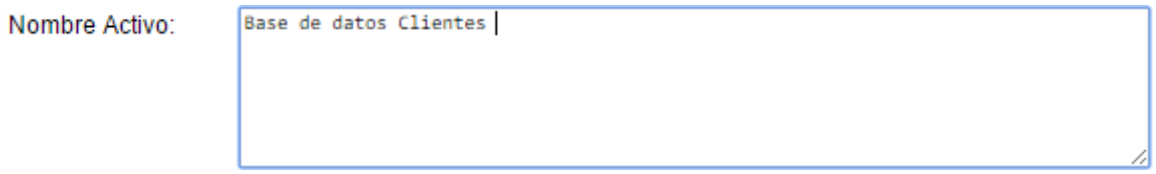
15. COMPONENTES FORMULARIO ACTIVOS

Al editar la información de un activo se puede seleccionar de una lista desplegable El dueño del proceso que tiene a cargo el activo de información que se esté editando en este momento. Esta lista ha sido ingresada al sistema en el formulario Cargo. Véase figura 29

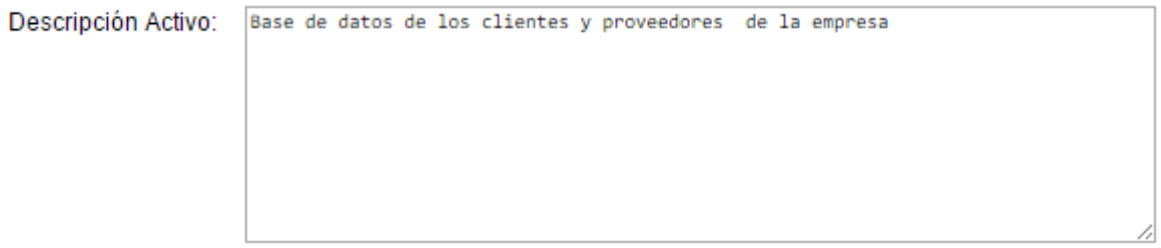
Figura 29 Componentes formulario activos



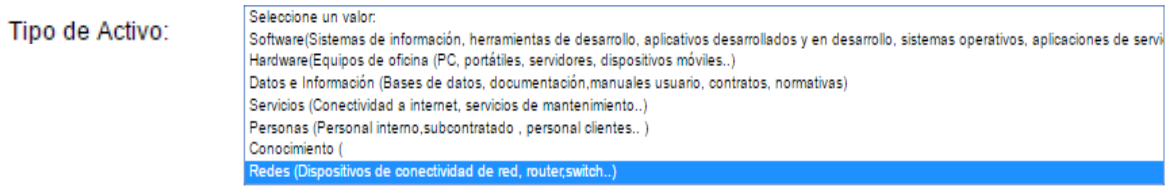
En este cuadro de texto debe ingresar el nombre del activo de información



En este cuadro de texto debe ingresar la descripción del activo de información



En esta lista desplegable debe seleccionar el tipo de activo según la metodología Magerit en el análisis y gestión de riesgos de los Sistemas de Información.

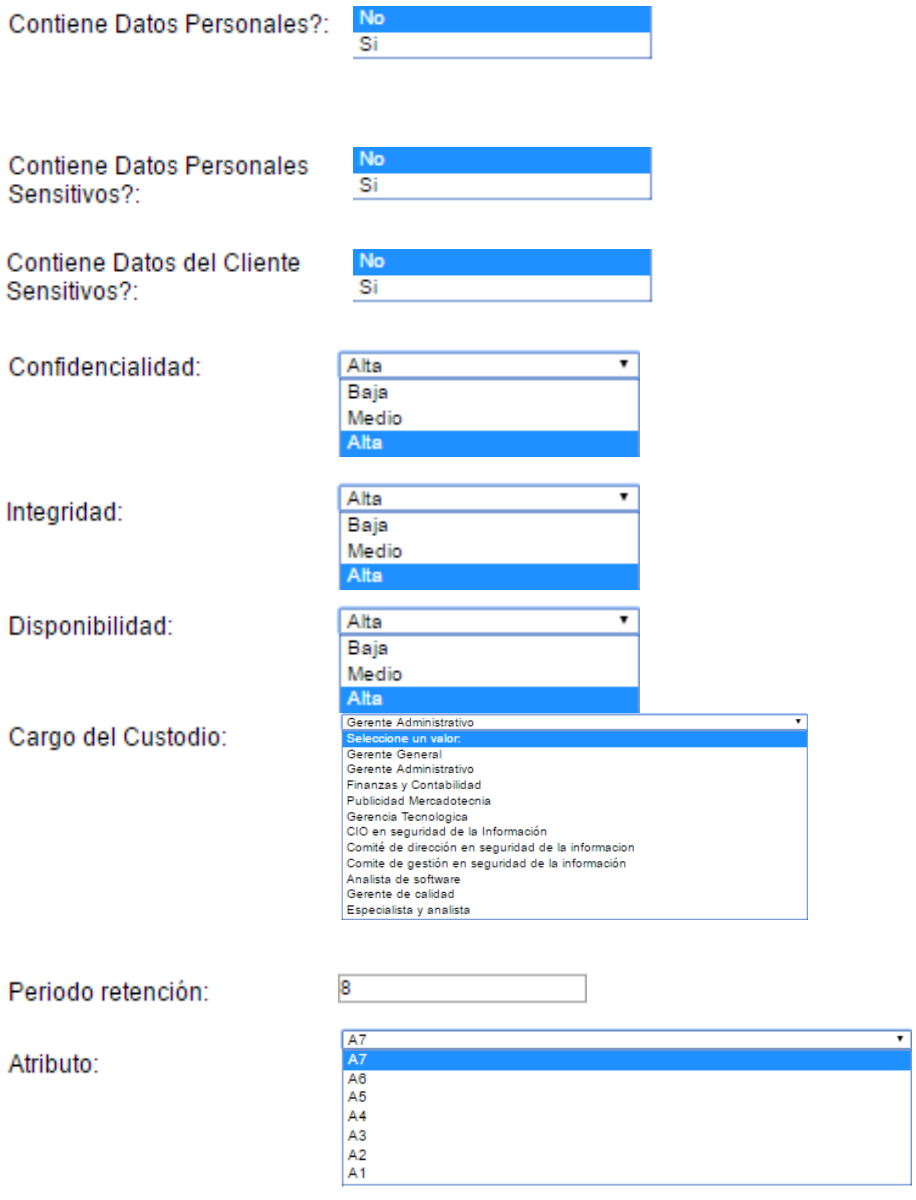


Fuente. Autores

15.1 EXPLICACIÓN FORMULARIO ACTIVOS

Al editar la información de un activo se puede seleccionar de una lista desplegable El dueño del proceso que tiene a cargo el activo de información que se esté editando en este momento. Esta lista ha sido ingresada al sistema en el formulario Cargo. Véase figura 30

Figura 30 Formulario activos

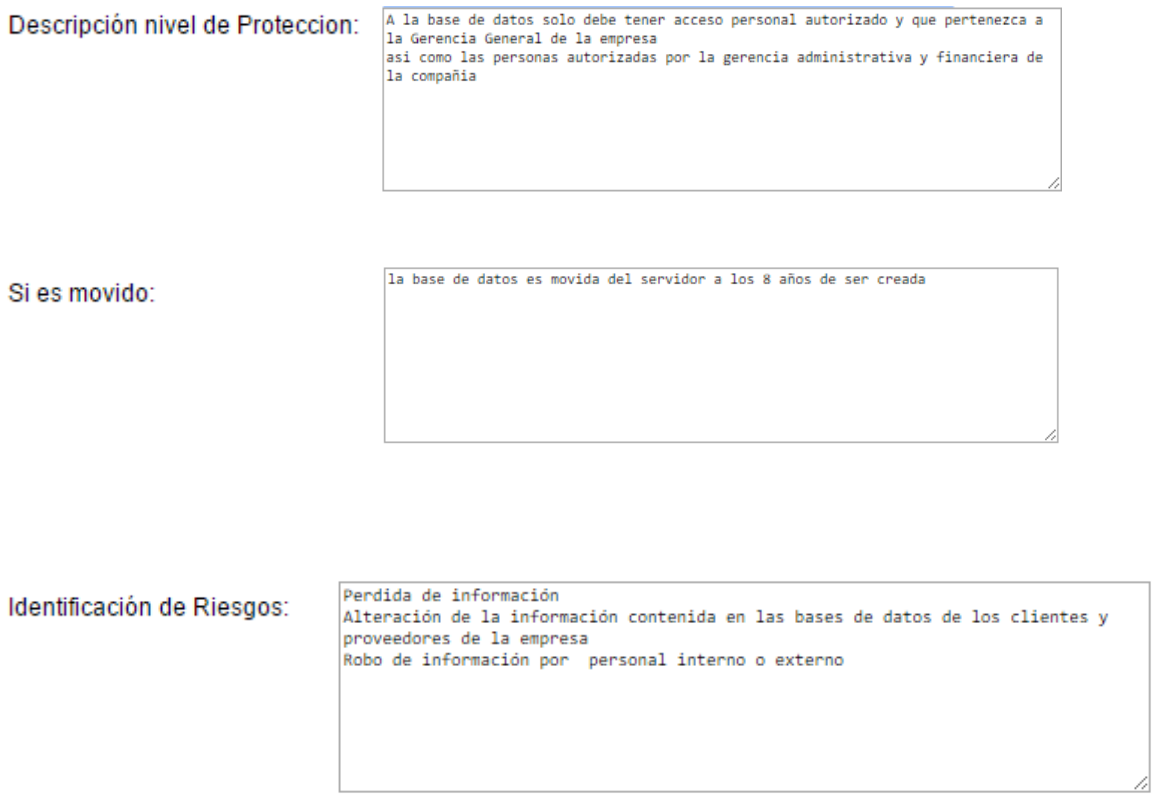


Fuente. Autores

15.2 EXPLICACIÓN FORMULARIO ACTIVOS

Al editar la información de un activo se puede seleccionar de una lista desplegable El dueño del proceso que tiene a cargo el activo de información que se esté editando en este momento. Esta lista ha sido ingresada al sistema en el formulario Cargo. Véase figura 31

Figura 31 Explicación formulario activos

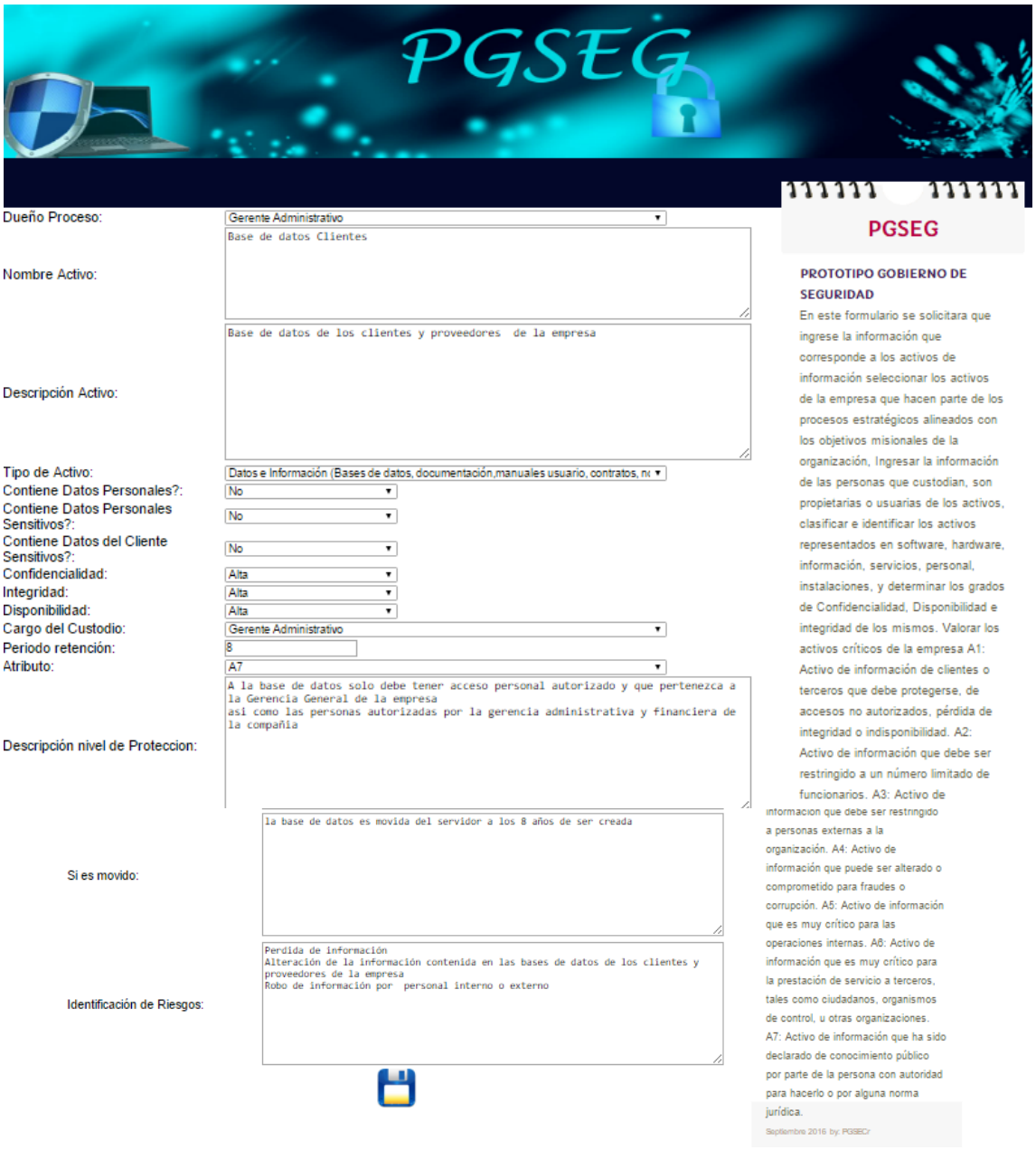


Fuente. Autores

16. COMPONENTES FORMULARIO ACTIVO

En este formulario se debe ingresar la información correspondiente a la identificación de los activos de información de la empresa. Véase figura 32

Figura 32 Componentes formulario activo



Fuente. Autores

17. COMPONENTES FORMULARIO OBJETIVO DE SEGURIDAD

Para ingresar la información en este formulario debe ir al menú que dice Contexto Empresarial buscar el enlace que dice objetivos seguridad, al hacer clic sobre este enlace se cargara el formulario correspondiente. Ver figura 33.

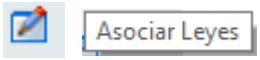
Explicación de los iconos encontrados en el formulario

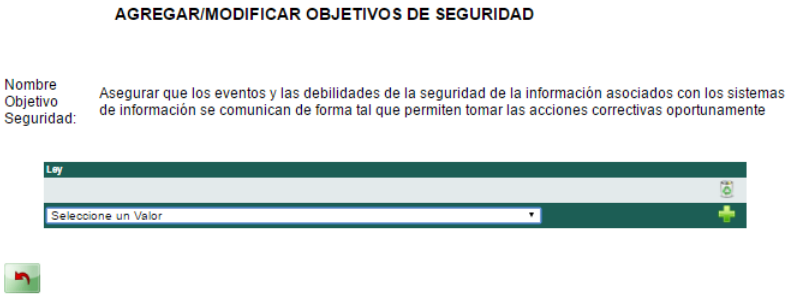
Figura 33 Formulario objetivo de seguridad

Edita la información de un registro.

Elimina un registro de la base de datos y de la grilla.

Adiciona un nuevo registro a la grilla





Adición de un registro en la base de datos.

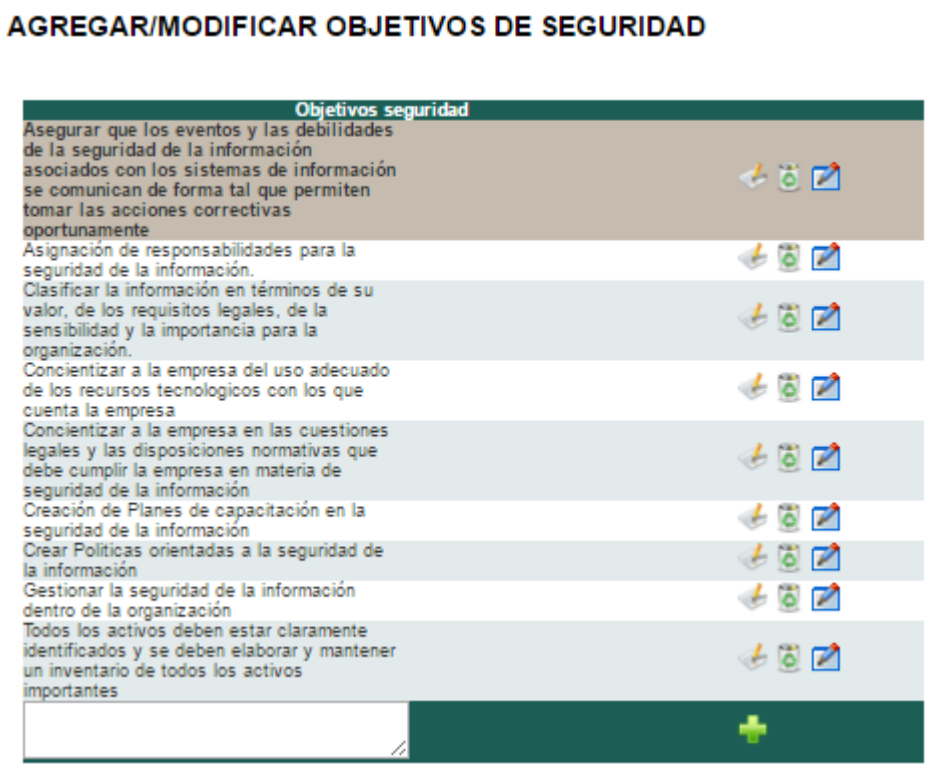
Lista desplegable administrable de las leyes del pais en seguridad de la información

Fuente. Autores

17.1 FORMULARIO OBJETIVO DE SEGURIDAD.

Una vez ingresada la información en el formulario se ve reflejada en la grilla tal como se puede observar en la figura 34.

Figura 34 Formulario objetivo de seguridad

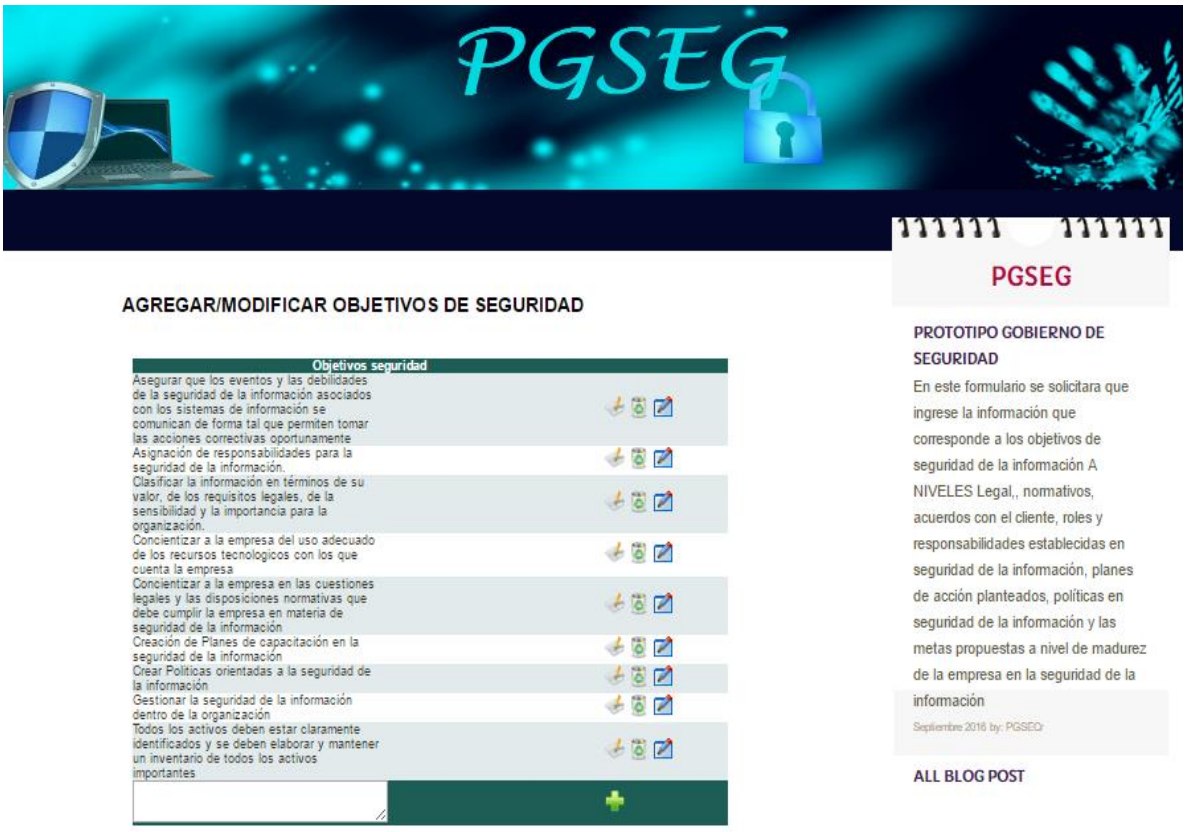


Fuente. Autores

17.2 FORMULARIO OBJETIVO DE SEGURIDAD.

En este formulario se debe ingresar la información de los objetivos de seguridad que la empresa debe adoptar. Esto se puede observar en la figura 35.

Figura 35 Formulario objetivo de seguridad



Fuente. Autores

18. COMPONENTES DEL FORMULARIO POLÍTICAS DE SEGURIDAD

Para ingresar la información en este formulario debe ir al menú que dice Contexto Empresarial buscar el enlace que dice políticas seguridad, al hacer clic sobre este enlace se cargara el formulario correspondiente. Ver figura 36

Explicación de los iconos encontrados en el formulario

Figura 36 Formulario políticas de seguridad

Edita la información de un registro.

Elimina un registro de la base de datos y de la grilla.

Adicionar Politica: Adiciona un nuevo registro a la grilla

Presentación de la grilla en el Formularios Políticas de Seguridad

Fuente. Autores

18.1 FORMULARIO POLÍTICAS DE SEGURIDAD.

En este formulario se debe ingresar la información de las políticas de seguridad propuestas para ser aprobadas por los altos directivos de la empresa. Ver figura 37

Figura 37 Formulario políticas de seguridad

Fuente. Autores

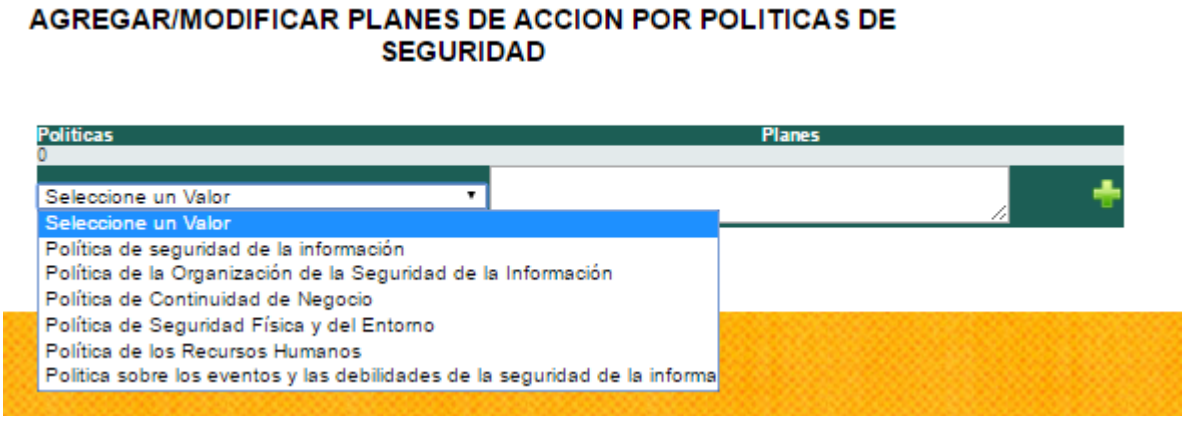
19. FORMULARIO PLANES DE ACCIÓN

Para ingresar la información en este formulario debe ir al menú que dice Contexto Empresarial buscar el enlace que dice planes de acción, al hacer clic sobre este enlace se cargara el formulario correspondiente. En la figura 38 se pueden observar una breve explicación de los iconos encontrados en el formulario

Figura 38 Formulario planes de acción

 Adiciona un nuevo registro a la grilla

Presentación de la grilla en el Formularios Políticas de Seguridad

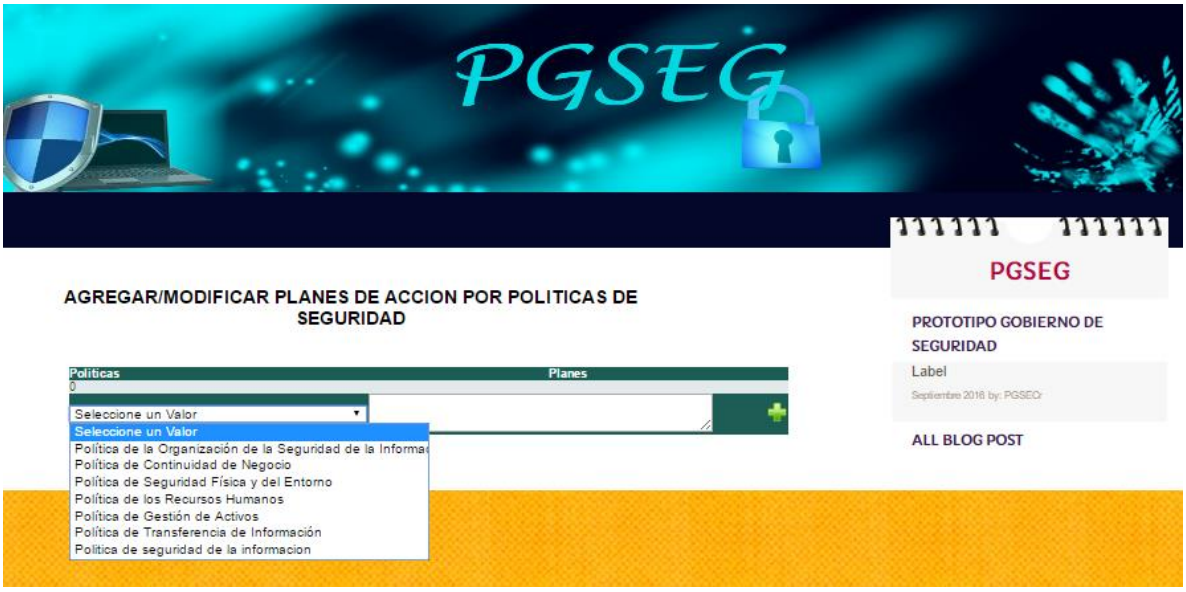


Fuente. Autores

19.1 FORMULARIO PLANES DE ACCIÓN

En este formulario se debe ingresar la información correspondiente a los planes de acción en seguridad que la empresa debe adoptar en beneficio de mejorar o instaurar un gobierno de seguridad de la información. Ver figura 39

Figura 39 Formulario planes de acción



Fuente. Autores

20. FORMULARIO ESTRATEGIAS DE SEGURIDAD

Para ingresar la información en este formulario debe ir al menú que dice Contexto Empresarial buscar el enlace que dice estrategias de seguridad, al hacer clic sobre este enlace se cargara el formulario correspondiente. Ver figura 40

Explicación de los iconos encontrados en el formulario

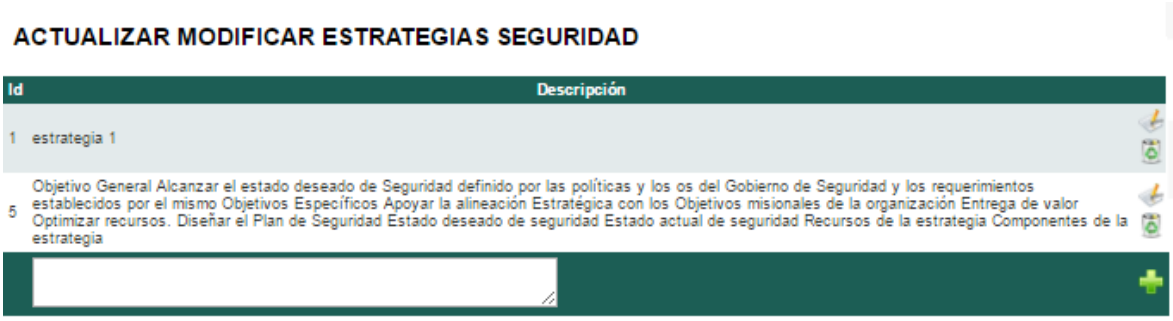
Figura 40 Formulario estrategias de seguridad

 Edita la información de un registro.

 Elimina un registro de la base de datos y de la grilla.

 Adiciona un nuevo registro a la grilla

Presentación de la grilla en el Formularios Estrategias de Seguridad



Fuente. Autores

20.1 FORMULARIO ESTRATEGIA

En este formulario se debe ingresar la información correspondiente a las estrategias que la empresa debe asumir en beneficio de un adecuado gobierno de seguridad de la información. Véase figura 41

Figura 41 Formulario estrategia

Fuente. Autores

21. FORMULARIO PARÁMETROS TIPO SEDES

Para ingresar la información en este formulario debe ir al menú que dice Parámetros buscar el enlace que dice tipos sedes, al hacer clic sobre este enlace se cargara el formulario correspondiente.
Véase eexplicación de los iconos encontrados en el formulario en la figura 42

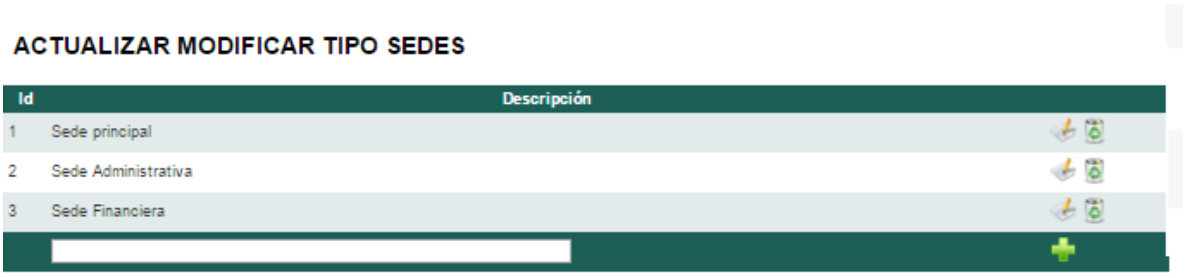
Figura 42 Formulario parámetros tipos sedes

 Edita la información de un registro.

 Elimina un registro de la base de datos y de la grilla.

 Adiciona un nuevo registro a la grilla

Presentación de la grilla en el Formulario Parametros Tipo Sede



Fuente. Autores

22. FORMULARIO PARÁMETROS PAÍSES

Para ingresar la información en este formulario debe ir al menú que dice Parámetros buscar el enlace que dice países, al hacer clic sobre este enlace se cargara el formulario correspondiente. Véase explicación de los iconos encontrados en el formulario en la figura 43

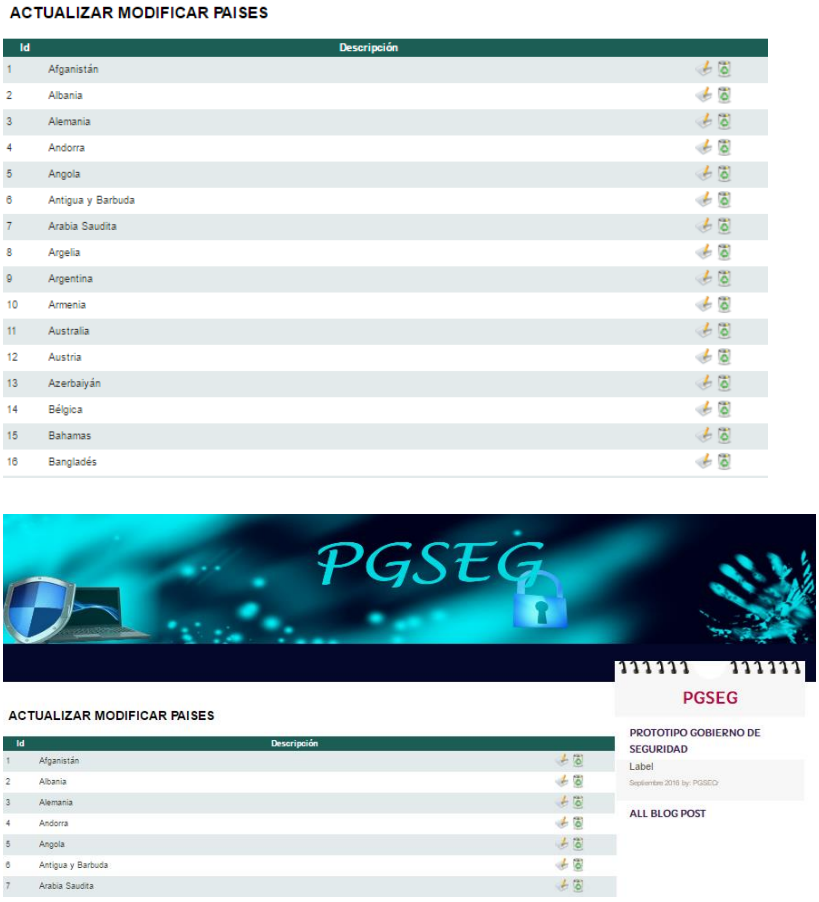
Figura 43 Formulario parámetros países

 Edita la información de un registro.

 Elimina un registro de la base de datos y de la grilla.

 Adiciona un nuevo registro a la grilla

Presentación de la grilla en el Formulario Parametros Paises



Fuente. Autores

23. FORMULARIO PARÁMETROS DEPARTAMENTOS

Para ingresar la información en este formulario debe ir al menú que dice Parámetros buscar el enlace que dice departamentos, al hacer clic sobre este enlace se cargara el formulario correspondiente. Véase la explicación de los iconos encontrados en el formulario en la figura 44

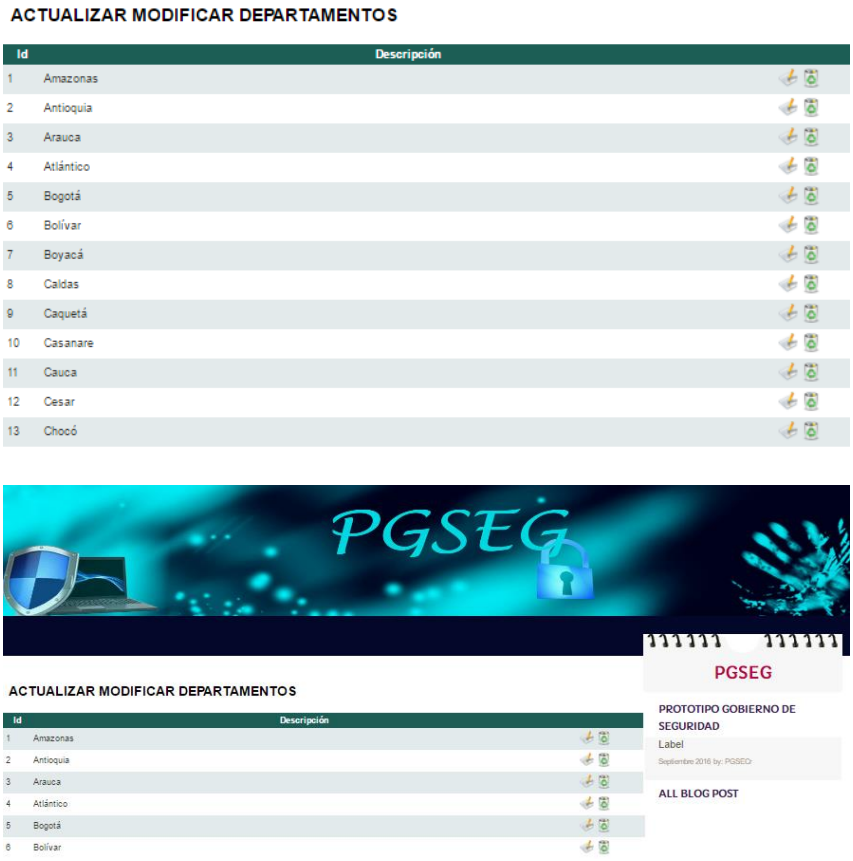
Figura 44 Formulario parámetros departamentos

 Edita la información de un registro.

 Elimina un registro de la base de datos y de la grilla.

 Adiciona un nuevo registro a la grilla

Presentación de la grilla en el Formulario Parametros Departamentos



Fuente. Autores

24. FORMULARIO PARÁMETROS CIUDADES

Para ingresar la información en este formulario debe ir al menú que dice Parámetros buscar el enlace que dice ciudades al hacer clic sobre este enlace se cargara el formulario correspondiente. Véase explicación de los iconos encontrados en el formulario en la figura 45

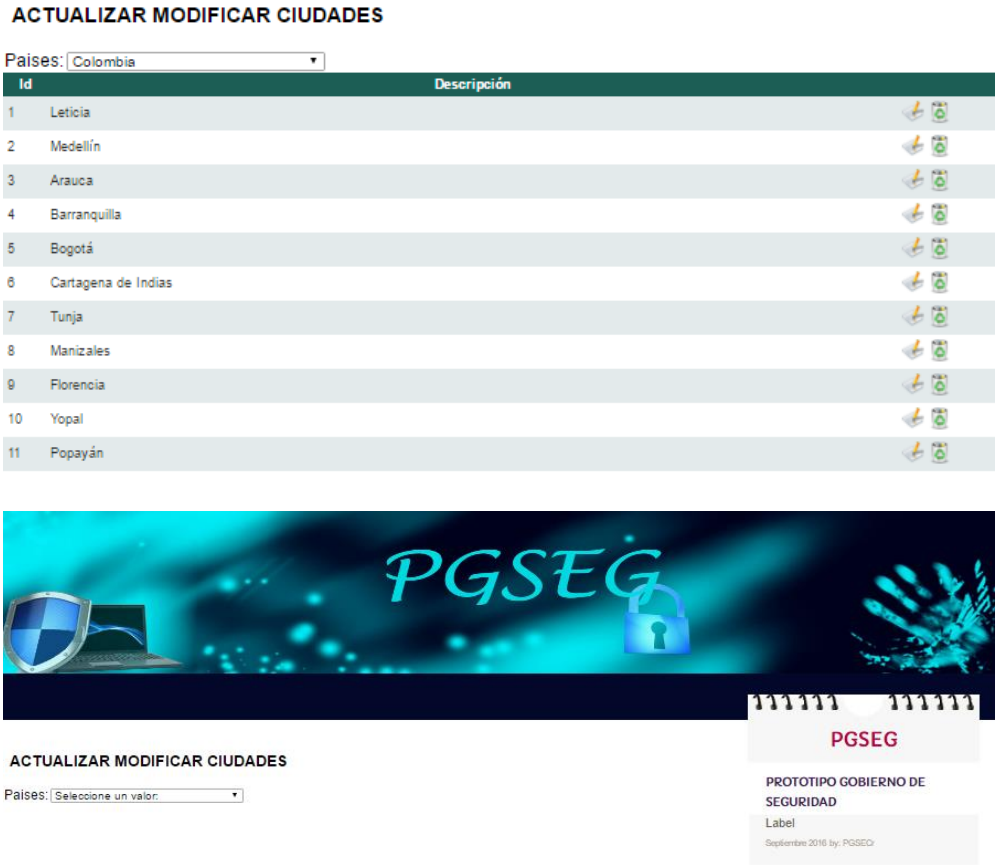
Figura 45 Formularios parámetros ciudades

 Edita la información de un registro.

 Elimina un registro de la base de datos y de la grilla.

 Adiciona un nuevo registro a la grilla

Presentación de la grilla en el Formulario Parametros Ciudades



Fuente. Autores

25. FORMULARIO ESTRATEGIA DA

Para ingresar la información en este formulario debe ir al menú que dice Dofa buscar el enlace que dice estrategia da al hacer clic sobre este enlace se cargara el formulario correspondiente. Véase explicación de los iconos encontrados en el formulario en la figura 46

Figura 46 Formulario estrategia da

 Edita la información de un registro.

 Elimina un registro de la base de datos y de la grilla.

 Adiciona un nuevo registro a la grilla

Presentación de la grilla en el Formulario Estrategia DA

Fuente. Autores

26. FORMULARIO ESTRATEGIA DO

Para ingresar la información en este formulario debe ir al menú que dice Dofa buscar el enlace que dice estrategia do al hacer clic sobre este enlace se cargara el formulario correspondiente. Véase explicación de los iconos encontrados en el formulario en la figura 47

Figura 47 Formulario estrategia do

 Edita la información de un registro.

 Elimina un registro de la base de datos y de la grilla.

 Adiciona un nuevo registro a la grilla

Presentación de la grilla en el Formulario Estrategia DO

Fuente. Autores

27. FORMULARIO ESTRATEGIA FA

Para ingresar la información en este formulario debe ir al menú que dice Dofa buscar el enlace que dice estrategia fa al hacer clic sobre este enlace se cargara el formulario correspondiente. Véase explicación de los iconos encontrados en el formulario en la figura 48

Figura 48 Formulario estrategia fa

 Edita la información de un registro.

 Elimina un registro de la base de datos y de la grilla.

 Adiciona un nuevo registro a la grilla

Presentación de la grilla en el Formulario Estrategia FA

Fuente. Autores

28. FORMULARIO ESTRATEGIA FO

Para ingresar la información en este formulario debe ir al menú que dice Dofa buscar el enlace que dice estrategia fo al hacer clic sobre este enlace se cargara el formulario correspondiente. Véase explicación de los iconos encontrados en el formulario en la figura 49

Figura 49 Formulario estrategia fo

 Edita la información de un registro.

 Elimina un registro de la base de datos y de la grilla.

 Adiciona un nuevo registro a la grilla

Presentación de la grilla en el Formulario Estrategia FO

Fuente. Autores

DISEÑO DE UN SOFTWARE PROTOTIPO QUE PERMITA PARAMETRIZAR UN GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN

Liana Carolina Montaña C, Diana Teresa Valencia Pedraza, Javier Alberto Montaña C.
Especialización en Seguridad Informática
Universidad Piloto de Colombia
Dirección Postal.
lianaweb@hotmail.com, valencia_diana@hotmail.com, ing.jmontanac@gmail.com.

***Resumen*- Este documento presenta el diseño de un software prototipo que brinde apoyo a las organizaciones que requieran implementar y parametrizar un Sistema de Gestión de Seguridad de la Información basado en el Gobierno de la Seguridad de la Información. El prototipo permitirá parametrizar los procesos, recursos, infraestructura de un gobierno de seguridad y abarcará hasta el reconocimiento de los activos críticos de información de las organizaciones.**

***Palabras Clave*- Gobierno de Seguridad, Gestión, Software, Activos críticos.**

I. INTRODUCCIÓN

Un gobierno de seguridad estructurado permitirá a cualquier organización tener un control adecuado de la información que maneja como también la identificación de los activos críticos de información los cuales son la base fundamental en la continuidad del negocio. Así mismo la organización podría identificar la gestión de riesgos y los controles para mitigar esos riesgos y de esta forma coadyuvar a las organizaciones a tomar las decisiones adecuadas y alinearlas con la misión y visión de la organización con el propósito de preservar los principios de confidencialidad (proteger los datos y la información intercambiada entre emisor y receptor frente a terceras personas), integridad (mantener los datos libres de modificaciones no autorizadas y la disponibilidad(asegura que se pueda acceder en cualquier momento a la información).[1]

En la medida que se vaya madurando la estructura del gobierno de seguridad dentro de la organización se puede ir planificando la inclusión de la inversión del presupuesto para la seguridad y satisfacer los recursos disponibles para las proyecciones de nuevas tecnologías basadas en seguridad todo alineado a la gestión del riesgo los objetivos organizacionales de los altos directivos.[2] Quienes tendrán una nueva manera de ver a la seguridad con un enfoque global que involucra infraestructura, personas y procesos.

II. DEFINICIÓN DEL PROBLEMA

Los altos directivos organizacionales piensan que con solo tener recursos tecnológicos a la mano están dándole flujo a la información, pero se olvidan que a esa información hay que protegerla como un activo crítico, tan es así que no le están dando el tratamiento adecuado y se percatan de ello en el momento en el cual la disponibilidad, integridad y confidencialidad de la información se ve comprometida y se obvian los marcos regulatorios estipulados por las leyes locales y regionales.

¿Qué les permitirá a los altos directivos organizacionales tomar adecuadas y acertadas decisiones misionales?

II.1 JUSTIFICACIÓN

Actualmente existe software especializado para el análisis de riesgos y escaneo de vulnerabilidades herramientas de hacking ético que asisten en la evaluación de la seguridad tanto de la información a distintos niveles como de los sistemas, redes de computadoras, aplicaciones Web y servidores, brindando ayuda a las organizaciones mediante pruebas de penetración (PenTest).[3] y exploración de dichos sistemas, con la finalidad de conocer los riesgos de las intrusiones. Estas herramientas y software son indispensables y han sido creados para dar continuidad al negocio. Aunque la base fundamental en una organización es la implementación estratégica y estructurada de un Gobierno de seguridad, actualmente no se tienen referencias de prototipos de software que planteen un SGSI desde el gobierno de Seguridad basado en los niveles de gestión, alineación estratégica

[1] Blog Seguridad informática martes 1 de noviembre de 2011 <http://seguridadanggie.blogspot.com.co/2011/11/confidencialidad.html>

[2] Lo que tienes que saber sección Magazine Impacto de las TI<http://informaticabasica28.blogspot.com.co/2013/03/impacto-de-las-ti.html>

[3]Instituto politécnico nacional herramientas para hacking ético Simulación de intrusión Test de penetración página 5. disponible desde Internet: <https://viclab.files.wordpress.com/2010/11/docfinal_pub.pdf>

organizacional, definición de roles y responsabilidades, normatividad y aspectos regulatorios, así como la administración de recursos. El estudio de investigación que se propone es la creación de un prototipo basado en el diseño y planificación de un gobierno de seguridad efectivo que sea la base fundamental para los procesos de continuidad del negocio.

II.2 ALCANCE

Por medio del análisis diseño y programación de un prototipo de software para la Gestión de gobierno de seguridad y con los conceptos regulatorios de las normas ISO 27001:2013[4], ISO 27014 ISACA en el dominio del gobierno de seguridad se pretende permitir a las organizaciones evaluar, controlar, dirigir y comunicar de forma eficiente las actividades que están relacionadas con la información. [5]

III. OBJETIVOS

III.1 OBJETIVO GENERAL

Diseñar un software prototipo que brinde apoyo a las organizaciones que requieran implementar y parametrizar un SGSI basado en el gobierno de la seguridad de la información.

III.2 OBJETIVOS ESPECÍFICOS

- Identificar las variables del gobierno de seguridad de la información basados en el manual de preparación al examen de CISM.
- Analizar los requerimientos de información que se necesitan para el establecimiento de un gobierno de seguridad de la información.
- Generar diagramas de casos de uso y flujogramas que permitan estructurar los procesos necesarios para establecer los flujos de entrada y salida de información en el software prototipo.
- Diseñar el modelo de base datos con el fin de estructurar las tablas, campos obligatorios, campos necesarios y consultas para facilitar el desarrollo del prototipo.
- Realizar el diseño y programación del prototipo
- Realizar las pruebas del prototipo con el propósito de identificar las posibles fallas que se puedan presentar y realizar los ajustes necesarios para su estabilización y puesta en funcionamiento.

Se presenta un esquema general modular que será nuestra base para estructurar el software prototipo que brinde apoyo a las organizaciones para implementar y parametrizar un SGSI basado en el gobierno de la seguridad de la información, un diagrama de flujo del sistema en general, un diagrama de los requerimientos técnicos del prototipo de software propuesto, diagramas de casos de uso que permiten identificar los actores que intervienen en el ingreso de información en el sistema, los diferentes casos de uso que describen los pasos o las actividades que deberán realizarse para llevar a cabo algún proceso dentro del sistema.

IV. DISEÑO METODOLÓGICO

Este proyecto se enmarca metodológicamente como proyecto de desarrollo tecnológico obteniendo como resultado un activo representado en un software prototipo y reportes que brinden apoyo a las organizaciones para implementar y parametrizar un SGSI basado en el gobierno de la seguridad de la información.

Analizando las variables que intervienen en el Gobierno de seguridad, hemos establecido unas directrices para estructurar el software prototipo basado en el gobierno de seguridad estándar para cualquier tipo de empresa y las normas internacionales ISO 27001:2013[6]- 27014 así como la proveniente de ISACA[7] en el dominio de Gobierno de Seguridad de la información.

Uno de los objetivos específicos para la propuesta de tesis es la de realizar el proceso de análisis de los requerimientos, diseño y programación del prototipo en lenguajes de programación orientada a objetos. Se propone para recopilar la información de forma ágil y organizada utilizar bases de datos en SQL server 2014 a su vez Diseñar una interfaz amigable utilizando herramientas de desarrollo de software que se ajusten a los requerimientos del prototipo para este fin se programara en .net framework 4.0 lenguaje c#.

Se ha pensado trabajar de manera modular el software prototipo de forma conjunta con las diferentes áreas que componen la estructura organizacional de una empresa, las personas que hacen parte del equipo de trabajo de cada una de ellas, los procesos de la organización, los recursos utilizados para el cumplimiento de los objetivos involucran diferentes

[4] INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Sistema de Gestión de la Seguridad de la Información. ISO/IEC 27001:2013. Bogotá D.C. 2013

[5] Blog especializado en sistemas de gestión de seguridad de la información Iso 2014 Gobernanza seguridad de la información 4 abril de 2014. disponible desde Internet: <http://www.pmg-ssi.com/2014/04/iso-27014-gobernanza-de-seguridad-de-la-informacion/>

[6] INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Sistema de Gestión de la Seguridad de la Información. ISO/IEC 27001:2013. Bogotá D.C. 2013

[7] ISACA. Manual de Preparación al Examen CISM 2014.Impreso en Estados Unidos de América. ISBN 978-1-60420-410-0

tipos de activos representados en datos, hardware, software, información, servicios, recursos entre otros.
Se sabe que el personal de la empresa tiene definidas sus funciones y conoce de antemano con qué recursos cuenta para poder realizar su trabajo diariamente, es por esto que a través de ellos se podrá recolectar la información ágilmente con eficiencia eficacia y efectividad obteniendo información actualizada y veraz que le permitirá al oficial de seguridad poder analizar la información y tomar decisiones acertadas para proponer mejoras en la seguridad de la información o para establecer un gobierno de seguridad de la información que involucre todas aquellas responsabilidades y prácticas que ejerce y aprueba la alta dirección de una empresa en cuanto a la seguridad de la información.

IV.1 IDENTIFICACIÓN DE VARIABLES DEL GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN

Para la mayoría de las organizaciones se ha constituido un gobierno corporativo como la estructura principal y se han establecido los objetivos de la empresa u organización, sin embargo, se ha obviado una rama del gobierno corporativo, como es el gobierno de seguridad de la información la cual se ha tenido que ir incorporando a medida que se ha tenido que responder acerca de las regulaciones legales y civiles.[8]

Un gobierno de seguridad efectivo debe tener en cuenta seis resultados básicos entre ellos se pueden mencionar[9]:

Alineación Estratégica
Gestión de Riesgos
Entrega de valor
Optimización de Recursos
Medición de Desempeño
Integración

IV.2 ANÁLISIS DE REQUERIMIENTOS DE INFORMACIÓN PARA ESTABLECER UN GOBIERNO DE SEGURIDAD

Basados en el Manual de Preparación al Examen CISM de ISACA en el dominio del Gobierno de seguridad de la información y en las variables identificadas se analizan los requerimientos de información necesarios que deben tener los formularios de la aplicación asi:

IV.2.1 Contexto Empresarial

En este formulario se solicitará información básica de la empresa se podrá incluir el logo corporativo, nombre de la empresa, seleccionar la actividad económica de una lista desplegable con información actualizada de la cámara de comercio, ingresar el nit de la empresa, el año de creación de la empresa con él se podrá llegar a obtener un acercamiento sobre el nivel de madurez de la empresa en cuanto a sus procesos. Datos misionales (misión visión y objetivos), así mismo se indagará acerca de las políticas empresariales que se tienen en seguridad de la información. Datos que serán indispensables para las siguientes fases de identificación y clasificación de los activos estratégicos de información de la empresa, siendo estos la base fundamental del software prototipo planteado.

.

- Nombre de la empresa
- Nit
- Año de creación de la empresa
- Número de empleados
- Misión
- Visión
- Objetivo general
- Políticas empresariales en seguridad de la información.

IV.2.2 Análisis DOFA

Una vez recolectada la información de la empresa, se realiza un análisis DOFA en seguridad de la información, este análisis va a permitir identificar los problemas Internos y externos de la organización, las debilidades, las fortalezas y las oportunidades, de esta forma se llegaría a tener un esquema preliminar de una gestión de riesgo que al sumarla al inventario de activos de información podria mostrar una perspectiva general sobre el proceder de los cumplimientos legales y una posible afectación económica.

IV.2.2.1 Fortalezas

Las empresas deben evaluar los puntos fuertes de su sistema de información. Esto incluye temas como la evaluación de la eficacia de los cortafuegos, configuración/ajustes de contraseña y protocolos de transferencia de información. Muchos programas de productividad en el lugar de trabajo "off theshelf" (fuera de la plataforma) tales como Microsoft Office e Internet Explorer vienen con una función de protección de seguridad. Sin embargo, las grandes empresas con múltiples ubicaciones a menudo tienen que ir mucho más allá de las soluciones "off the shelf" (fuera de la plataforma).[10]

[8] ISACA. Manual de Preparación al Examen CISM 2014.Impreso en Estados Unidos de América. ISBN 978-1-60420-410-0

[9] ISACA. Manual de Preparación al Examen CISM 2014.Impreso en Estados Unidos de América. ISBN 978-1-60420-410-0

[10] Análisis FODA de Seguridad, Dwight Chestnut. Disponible en Internet: www.ehowenespanol.com/analisis-foda-seguridad-sobre_145898//

IV.2.2.2 Debilidades

Las empresas deben evaluar con realismo las debilidades de sus sistemas de seguridad de IT. Las debilidades típicas se presentan en forma de violaciones de seguridad de los empleados, robo de los empleados y protocolos de transferencia de información defectuosos. Incluso la falta de fondos puede ser una debilidad porque las empresas no tienen el capital operativo necesario para solucionar correctamente una vez que las principales debilidades sean detectadas.[11].

IV.2.2.3 Oportunidades

Representadas en las opciones que el mercado ofrece para la seguridad de la información, leyes, normas, capacitaciones, tecnologías, servicios entre otros.

IV.2.2.4 Amenazas

Ataques de seguridad que se originan fuera de la empresa. El ejemplo más común es un ataque de un pirata o un virus informático distribuido masivamente.[12]

IV.2.3 ANÁLISIS POR PROCESOS

Teniendo como base los objetivos misionales del negocio se propone realizar el levantamiento de la información a niveles de objetivos por cada área de la empresa para ello se debe analizar la información que se maneja por áreas, así como los procesos misionales que maneja la organización, las personas involucradas en los procesos y los recursos que utilizan para su labor diaria, información que será ingresada al sistema por las personas que hacen parte del equipo de trabajo de cada área de la empresa, de esta forma se podrán identificar los roles, responsabilidades y recursos utilizados para cumplir los objetivos del área alineados con los objetivos misionales de la empresa. Así mismo se propondrán encuestas orientadas a un ambiente de seguridad de información dentro de sus áreas de trabajo y a nivel empresarial las cuales pueden permitirla identificación de huecos de seguridad y o vulnerabilidades en las diferentes áreas o procesos.

IV.2.4 Identificación de activos de información críticos

Se obtendrá de cada área de la organización la descripción de los activos de información que son críticos para cada proceso, describiendo el tipo de activo, así como todas las acciones o medidas necesarias para garantizar el cumplimiento de sus objetivos, entre los que se deben encontrar la seguridad de la información entre otros, determinado a través de la información suministrada las propuestas de una clasificación y valores de los mismos, con el fin de determinar para la organización un análisis de riesgo preliminar identificando los atributos que se debe tener en cuenta para la protección del activo de información.

Con la información recolectada en el contexto empresarial, el análisis de los procesos y la evaluación de los activos a niveles de confidencialidad, integridad y disponibilidad se llega a identificar cuales activos son críticos para la organización y cuales necesitan un nivel de seguridad más estricto. Así mismo la certificación de NTC-ISO9001 en calidad y gestión de calidad que ha sido implementada en algunas organizaciones permitirá obtener un detalle más preciso de los activos de información que intervienen en los procesos críticos de las empresas y a su vez identificar los riesgos que pueden causar perdida del objetivo misional de la estrategia de la organización. No obstante, es importante realizar una clasificación de la información en pública, privada, semiprivada, confidencial y especificar los medios de almacenamiento de dicha información, asignar roles y responsables de la misma y los recursos utilizados para su resguardo y tratamiento.

IV.2.5 Objetivos de Seguridad

Una vez se establezcan cuáles son los objetivos de negocio se propone el establecimiento de los objetivos de seguridad los cuales deben estar alineados estratégicamente con los objetivos del negocio basándose en las normas regulatorias a niveles de seguridad y marcos legales. Cuatro ítems son de vital importancia para plantear los objetivos de seguridad[13] **Organización** (Matriz RACI) Roles y responsabilidades a nivel de seguridad de la información, **planes** (Acciones, responsables, administración adecuada de recursos), **políticas** de seguridad teniendo en cuenta la norma **ISO 27001:2013**, **metas** a niveles de madurez en seguridad de la información. [14]

Para el establecimiento d**e las políticas** se toma un modelo estándar basado en la norma ISO 27001:2013 así:

- Política de Seguridad de la Información
- Política de la Organización de la Seguridad de la Información
- Política de Continuidad de Negocio
- Política de Seguridad Física y del Entorno
- Política de los Recursos Humanos
- Política de Gestión de Activos
- Política de Control de Acceso
- Política de Seguridad de Operaciones
- Política de Seguridad de las Comunicaciones

[11] Ibíd.

[12] Ibíd

[13] ISACA. Manual de Preparación al Examen CISM 2014.Impreso en Estados Unidos de América. ISBN 978-1-60420-410-0

[14] ISACA. Manual de Preparación al Examen CISM 2014.Impreso en Estados Unidos de América. ISBN 978-1-60420-410-0

- Política de Transferencia de Información
- Política Relaciones con los Proveedores
- Política de Gestión de Incidentes de Seguridad de la Información
- Política de Cumplimiento

IV.2.6 Planes de Seguridad

Por último, se plantean los flujos de procesos por áreas y los planes de seguridad, estos últimos nos permiten identificar los responsables de la seguridad en la organización, las acciones que se deben llevar a cabo para que se cumplan los objetivos de seguridad estipulados, los recursos utilizados para su establecimiento y los tiempos en los cuales se deben llevar a cabo todas las labores para el establecimiento de la seguridad de la información en la empresa.

IV.2 DIAGRAMA DE FLUJO Y CASOS DE USO

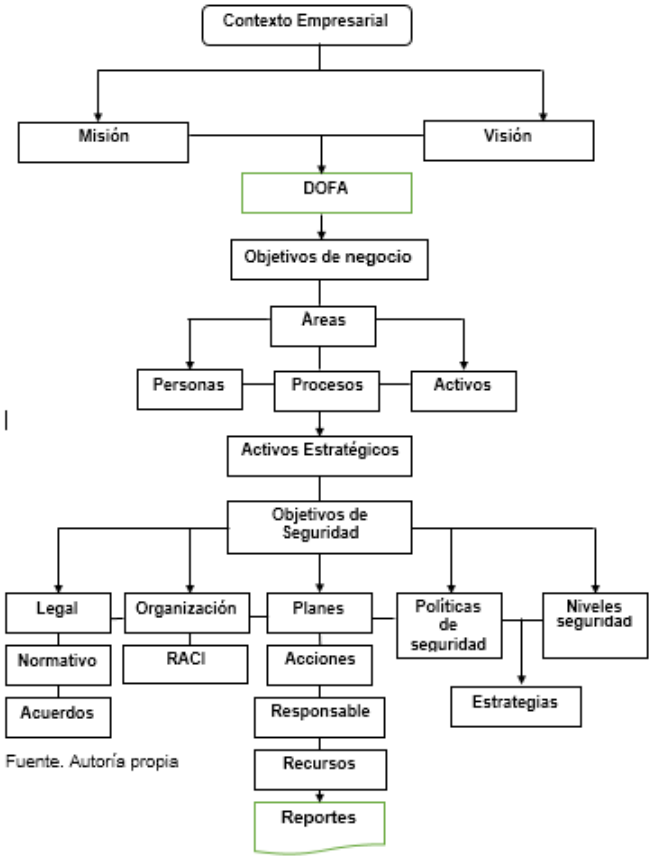


Fig. 1 Diagrama de Flujo y Casos de Uso

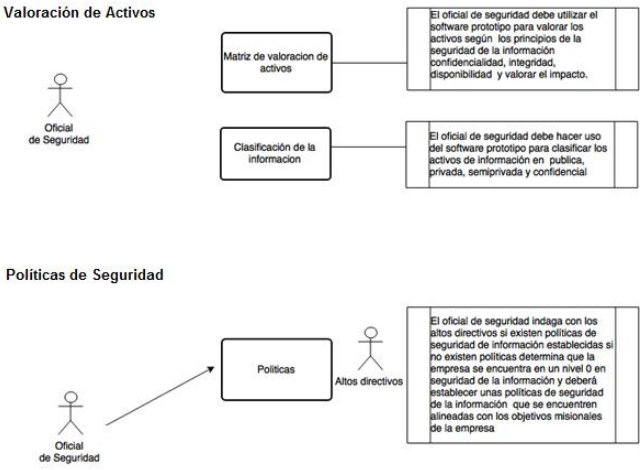


Fig.2 Casos de uso, datos generales y estructura organizacional

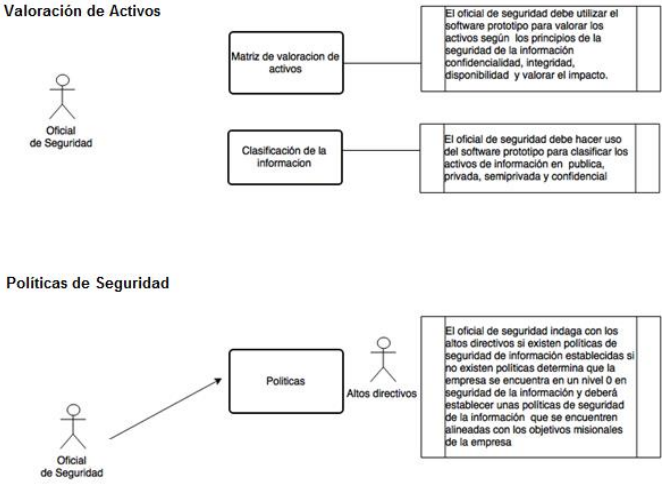


Fig.3 casos de uso valoración de activos y políticas de seguridad

IV.3 MODELO ENTIDAD RELACION BASE DE DATOS

El primer paso en el diseño de una base de datos relacional es la creación de la base datos, la configuración de cada una de las tablas (Entidades), la programación de los procedimientos almacenados (create, read, update, delete) y el establecimiento de las claves primarias y foráneas de las entidades. Por último, la identificación de las relaciones entre las entidades a través de sus llaves. A continuación, se describirán las entidades creadas en el desarrollo del proyecto y se enumerarán los procedimientos almacenados programados de acuerdo a las especificaciones funcionales que el software demanda.

IV.3.1 Entidades

Un objeto no es más que un conjunto de variables (o datos) y métodos (o funciones) relacionados entre sí. Los objetos en programación se usan para modelar objetos o entidades del mundo real. Un objeto es, por tanto, la representación en un programa de un concepto, y contiene toda la información

necesaria para abstraerlo: datos que describen sus atributos y operaciones que pueden realizarse sobre los mismos.14

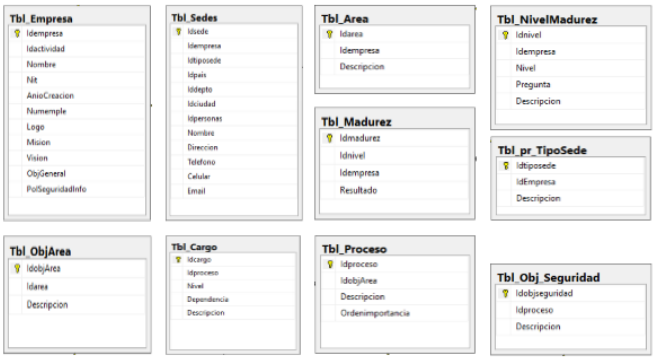


Fig. 4 Entidades

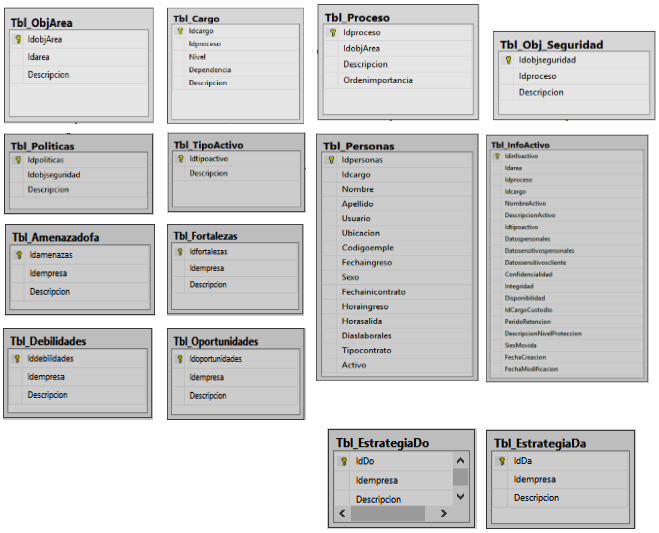


Fig. 5 Entidades definidas en la base de datos

IV.3.2 Procedimientos Almacenados

Conjunto de comandos que pueden ser ejecutados directamente en el servidor, es decir, será ejecutado por el servidor de Base de Datos y no por el programa cliente que lo accede, permitiendo la ejecución de una acción o conjunto de acciones específicas.[15]

Usar procedimientos almacenados en lugar de concatenación de cadenas para construir consultas dinámicas desde los datos de entrada del usuario para todas las sentencias SQL reduce la posibilidad de ataques de inyección SQL.[16]

En el diseño de la base de datos del software prototipo se programaron diferentes procedimientos almacenados para el ingreso de información, consulta, modificación y eliminación de la misma. A continuación, se realiza una corta descripción de los procedimientos almacenados.

IV.3.2.1 Procedimiento Almacenado Consultar

En la figura 6 se pueden observar los procedimientos almacenados creados para realizar las diferentes consultas de datos, que se realizan a sus respectivas tablas. Estos procedimientos almacenados devuelven los registros de cada una de las tablas

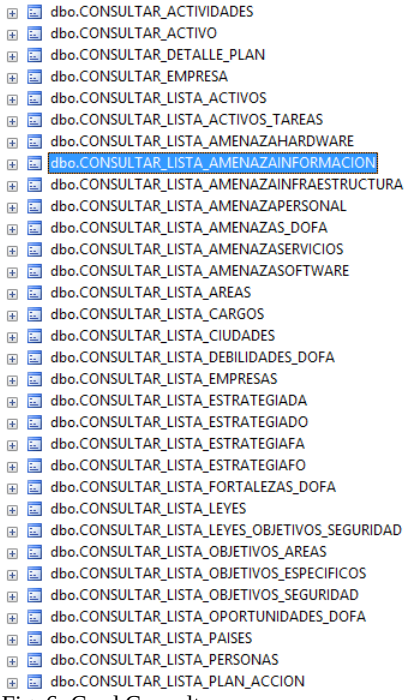


Fig. 6: Crud Consultar

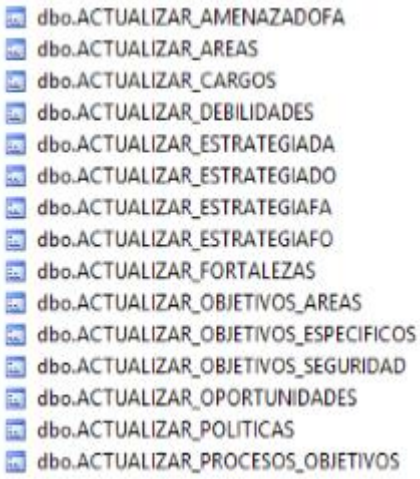


FIG. 6 Crud Actualizar

[14] http://luis.izqui.org/resources/ProgOrientadaObjetos.pdf
[15] https://www.ecured.cu/Procedimientos_almacenados
[16] http://www.sqlshack.com/es/creando-usando-procedimientos-almacenados-crud/

IV.3.2.2 Procedimiento Almacenado Actualizar

En la figura 7 se pueden observar los procedimientos almacenados creados para realizar las diferentes consultas de actualización de datos. Serán utilizados para actualizar la información de los registros existentes en las diferentes tablas

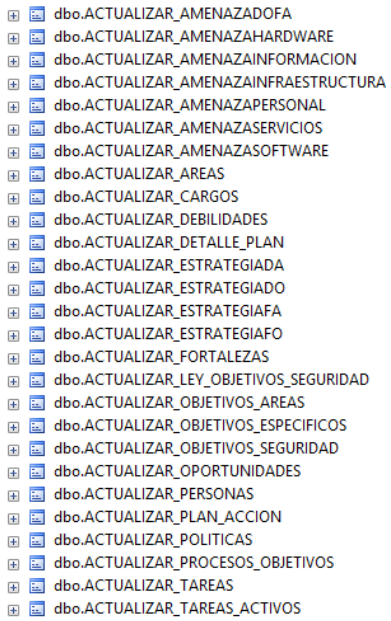


Fig. 7 Crud Actualizar

IV.3.2.2 Procedimiento Almacenado Eliminar

En la figura 8 se pueden observar los procedimientos almacenados creados para realizar las diferentes consultas de eliminación de datos. Con ellos se pretende eliminar un registro de una determinada tabla en la base de datos.

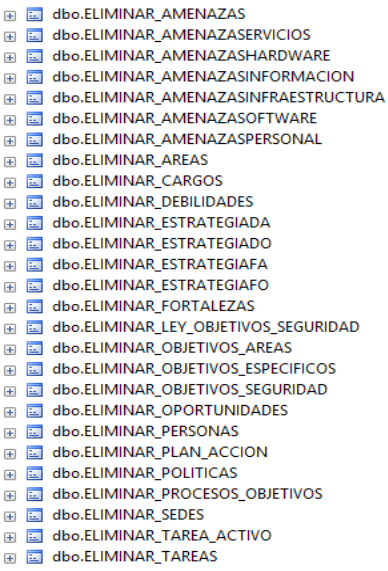


Fig. 8 Crud Eliminar

IV.4 DISEÑO DEL PROTOTIPO Y ARQUITECTURA DEL SOFTWARE

En la fase de diseño del prototipo se plasman los requerimientos en forma de código de programación y se diseña una interfaz sencilla, pero practica a la hora de modelar la estructura funcional del software. Para ello se programa el prototipo con el software visual studio .net lenguaje C# y base de datos Sqlserver 2014. En la programación orientada a objetos (POO), un objeto viene siendo la representación en un programa de un concepto y contiene toda la información necesaria para abstraerlo, son datos que describen sus atributos y operaciones que se pueden realizar sobre los mismos.[17] La arquitectura del software planteado para el diseño del prototipo se basa en el modelo por capas y entidades así:

- Capa de negocio: con lleva la lógica de negocio
- Capa de datos: se maneja la información de la base de datos
- Capa de presentación: capa con la cual interactúan los usuarios
- Entidades manejo por objetos.

IV.4.1 Capa de Negocio

En la figura 9 se pueden observar las clases creadas para la capa de negocio. En ella se incluye toda la lógica de negocio de la aplicación

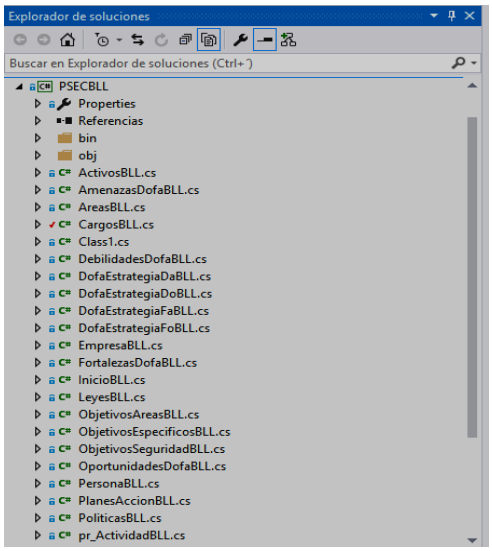


Fig. 9 Clases de la capa de Negocio

[17] http://luis.izqui.org/resources/ProgOrientadaObjetos.pdf

IV.4.1.1 Código de Programación Capa de Negocio

En la figura 10 se puede observar una parte del código de programación generado para la capa de negocio.

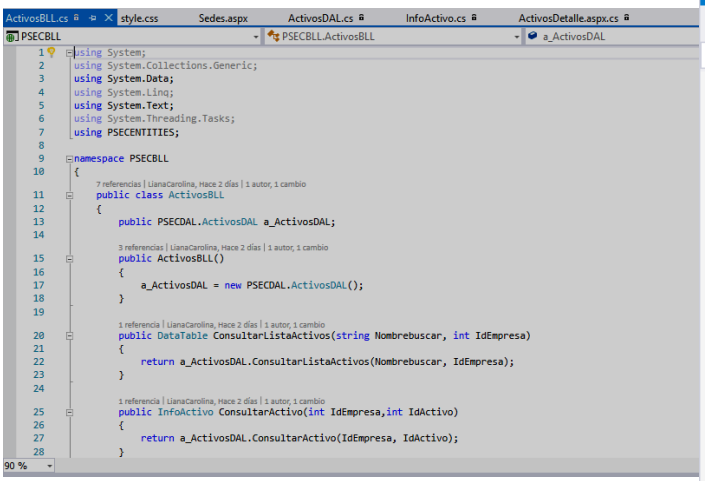


Fig.10 Código Capa de Negocio

IV.4.2 Capa de Datos

En la figura 11 se puede observar las clases creadas para la capa de datos. Tiene que ver con todo lo referente a la conexión con la base de datos y el llamado a los diferentes procedimientos almacenados.

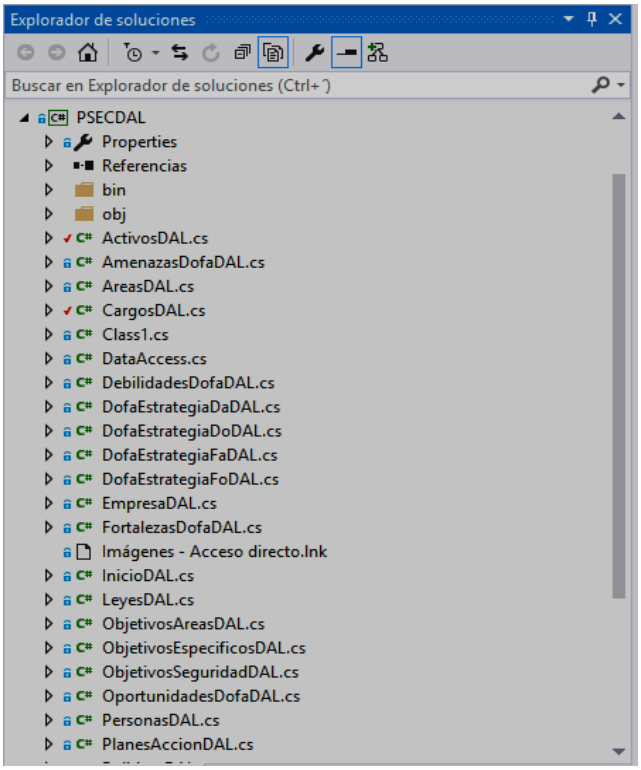


Fig. 11 Clases de la capa de datos

IV.4.2.1 Codigo de programación Capa de Datos

En la figura 12 se puede observar una parte del código de programación generado para la capa de datos.

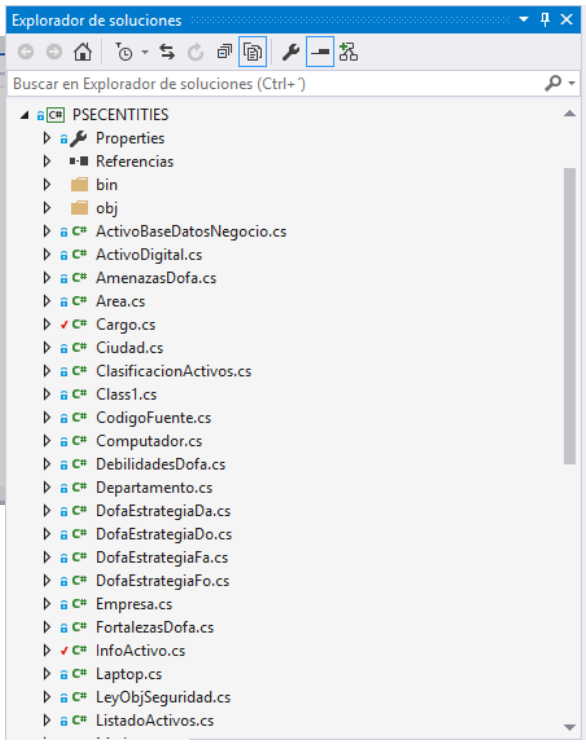


Fig. 12 Código de la capa de datos

IV.4.3 Capa de Presentación

En la figura 13 se puede observar las clases creadas para la capa de presentación. Hace referencia a la parte visual o lo que se le presenta al usuario final de la aplicación conocido también como Front-end.

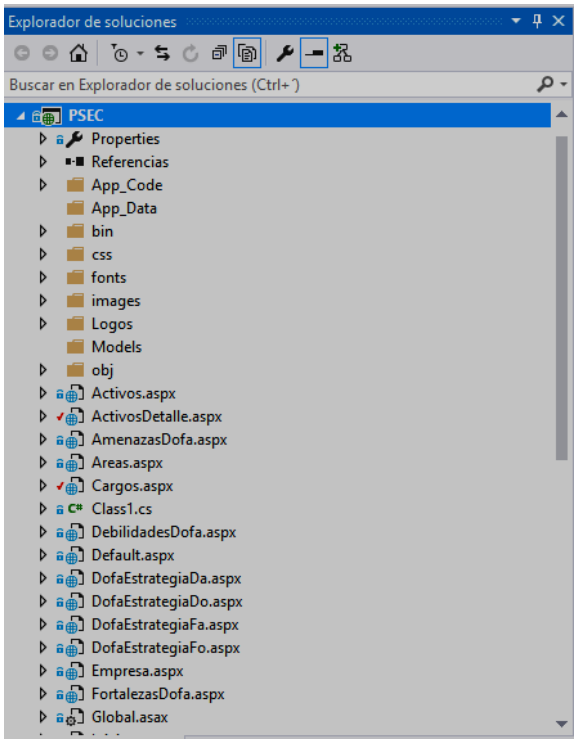


Fig. 13 Capa de presentación

IV.4.3.1 Código de programación capa de Presentación

En la figura 14 se puede observar una parte del código de programación generado para la capa de presentación.

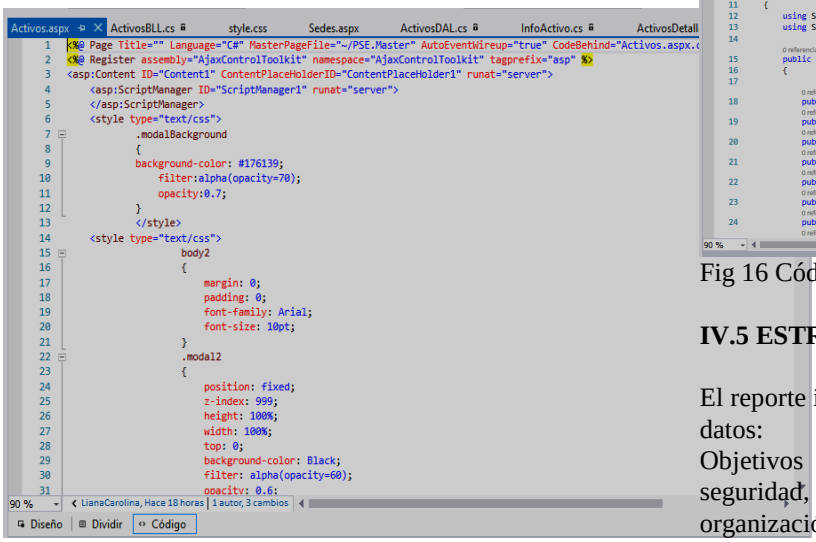


Fig. 14 Código capa de presentación

IV.4 Capa de Entidades

En la figura 15 se puede observar las clases creadas para la capa de entidades.

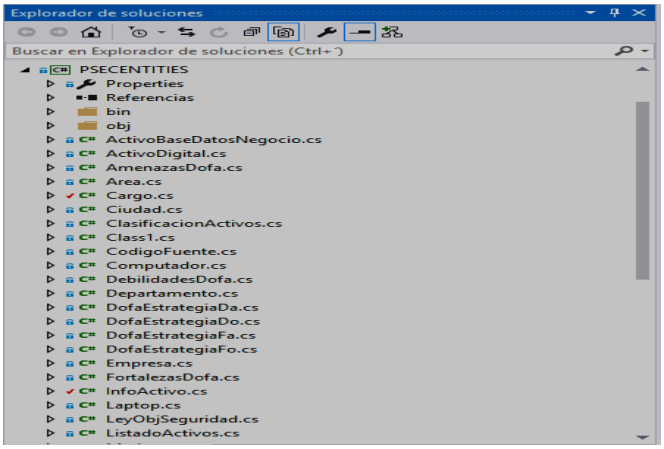


Fig. 15 Entidades

IV.4.1 Código de programación capa de Entidades

En la figura 16 se puede observar una parte del código de programación generado para la capa de entidades.

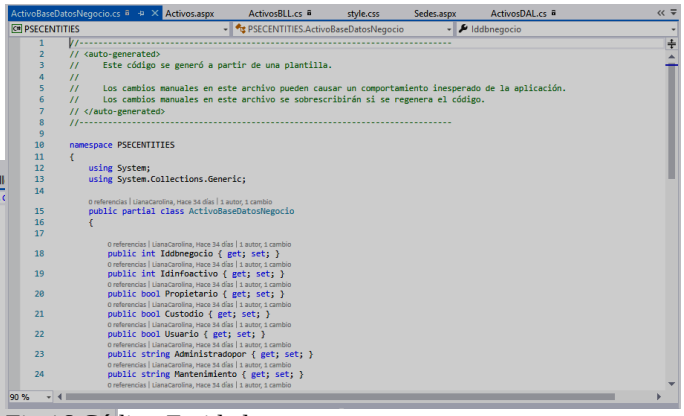


Fig 16 Código Entidades

IV.5 ESTRATEGIAS

El reporte involucra las siguientes consultas a nivel de base de datos:
Objetivos de Negocio, Objetivos de Seguridad, política de seguridad, relación de los recursos que cuenta la organización, el análisis de brecha de seguridad, estructura organizacional, roles y responsabilidades.

Informacion que se debe tener en cuenta para la definicion de la estrategia de seguridad.[18]

- Objetivos Especificos
- Relacion componentes, estrategico, tactico y operativo
- Analisis de brecha de seguridad
- Elementos de la estrategia
- Recursos
- Roles y responsabilidades
- Restricciones
- Implementación de la estrategia

IV.6 MEDICIONES DEL GOBIERNO DE SEGURIDAD

Durante la implementación del gobierno de seguridad, se debe realizar una medición del estado de la ejecución del gobierno de seguridad en la organización o empresa, por tal razón se plantea los siguientes formatos:

- Plan de capacitación y sensibilización
- Plan de auditorías Internas
- Plan de mejora continua
- Matriz Raci (encargado, responsable, consultado, informado)

V. CONCLUSIONES

Es viable la realización del software prototipo propuesto en la tesis, cumple con las expectativas de funcionalidad y

---

18 http://52.1.175.72/portal/sites/all/themes/argo/assets/img/Pagina/16-PlaneacionEstrategicaSeguridad.pdf

parametrización de gobierno de seguridad ya que ha sido formulado bajo los parámetros de las normas ISO 27001:2013 y el Manual de Preparación para el Examen CISM de ISACA en el dominio del gobierno de seguridad.

La propuesta de la tesis se sale de los estereotipos de realizar un análisis en seguridad de la información exclusiva para una sola empresa propuestas planteadas en otros proyectos de grado. Nuestra propuesta incluye la realización de un producto para recolectar y permitir estructurar un gobierno de seguridad de la información siendo esta la base para establecer un SGSI a nivel empresarial y el prototipo se propone no solo para el análisis de una empresa si no para cualquier empresa que quiera establecer un gobierno de seguridad de la información que sea transversal al gobierno corporativo de la organización o empresa.

La propuesta de software prototipo al ser modular en su estructura de diseño programación y a niveles funcionales puede llegar a extenderse en la programación futura hacia el análisis de riesgos en seguridad de la información y puede llegar a ser la base para el desarrollo de un módulo de continuidad del negocio.

El análisis de las variables propuestas en el Manual de Preparación al Examen de CISM por ISACA permitió estructurar mejor el software, así mismo nos enriqueció en conocimiento y experiencia replanteando la forma más adecuada de plasmar las ideas que se tenían para la programación del prototipo, tan es así que al inicio se planteó la posibilidad de asignar responsables en las empresas para ingresar solo la información adecuada al software, información que solo compete al establecimiento de las funciones de las personas en la empresa, luego de analizar bien las diversas situaciones que se podrían llegar a presentar al ingresar la información en el software prototipo se replanteo el esquema de utilización con el acompañamiento siempre del oficial de seguridad de la información por el conocimiento y experticia que da el valor agregado, esto con el fin de ser un apoyo y ayuda para plasmar los datos solicitados en términos de la seguridad de la información. Por esta misma razón la creación de las ayudas en el software para ingresar únicamente la información solicitada y obtener buenos resultados en los reportes finales.

VI. AGRADECIMIENTOS

El presente trabajo de investigación fue realizado bajo la supervisión de la Ing. Lorena Ocampo, y el apoyo del Ing. Juan Carlos Alarcón, a quien nos gustaría expresar nuestro más profundo agradecimiento por hacer posible la realización de este estudio, además de agradecer su paciencia, tiempo y dedicación.

VI. REFERENCIAS

[1] Blog Seguridad informática martes 1 de noviembre de 2011 <http://seguridadanggie.blogspot.com.co/2011/11/confidencialidad.html>

[2] Lo que tienes que saber sección Magazine Impacto de las TIhttp://informaticabasica28.blogspot.com.co/2013/03/impacto-de-las-ti.html

[3] Instituto politécnico nacional herramientas para hacking ético Simulación de intrusión Test de penetración página 5. Disponible en Internet: https://viclab.files.wordpress.com/2010/11/docfinal_pub.pdf

[4] INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Sistema de Gestión de la Seguridad de la Información. ISO/IEC 27001:2013. Bogotá D.C. 2013

[5] Blog especializado en sistemas de gestión de seguridad de la información Iso 2014 Gobernanza seguridad de la información 4 abril de 2014. disponible desde Internet: <http://www.pmg-ssi.com/2014/04/iso-27014-gobernanza-de-seguridad-de-la-informacion/>

[6] INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Sistema de Gestión de la Seguridad de la Información. ISO/IEC 27001:2013. Bogotá D.C. 2013

[7] ISACA. Manual de Preparación al Examen CISM 2014.Impreso en Estados Unidos de América. ISBN 978-1-60420-410-0

[8] ISACA. Manual de Preparación al Examen CISM 2014.Impreso en Estados Unidos de América. ISBN 978-1-60420-410-0

[9] ISACA. Manual de Preparación al Examen CISM 2014.Impreso en Estados Unidos de América. ISBN 978-1-60420-410-0

[10] Análisis FODA de Seguridad, Dwight Chestnut. Disponible en Internet: www.ehowenespanol.com/analisis-foda-seguridad-sobre_145898//

[11] Análisis FODA de Seguridad, Dwight Chestnut. Disponible en Internet: www.ehowenespanol.com/analisis-foda-seguridad-sobre_145898/

[12] ISACA. Manual de Preparación al Examen CISM 2014.Impreso en Estados Unidos de América. ISBN 978-1-60420-410-0

[13] ISACA. Manual de Preparación al Examen CISM 2014.Impreso en Estados Unidos de América. ISBN 978-1-60420-410-0

[14] http://luis.izqui.org/resources/ProgOrientadaObjetos.pdf

[15] https://www.ecured.cu/Procedimientos_almacenados

[16]http://www.sqlshack.com/es/creando-usando-procedimientos-almacenados-crud/

[17] http://luis.izqui.org/resources/ProgOrientadaObjetos.pdf

[18] http://52.1.175.72/portal/sites/all/themes/argo/assets/img/Pagina/16-PlaneacionEstrategicaSeguridad.pdf